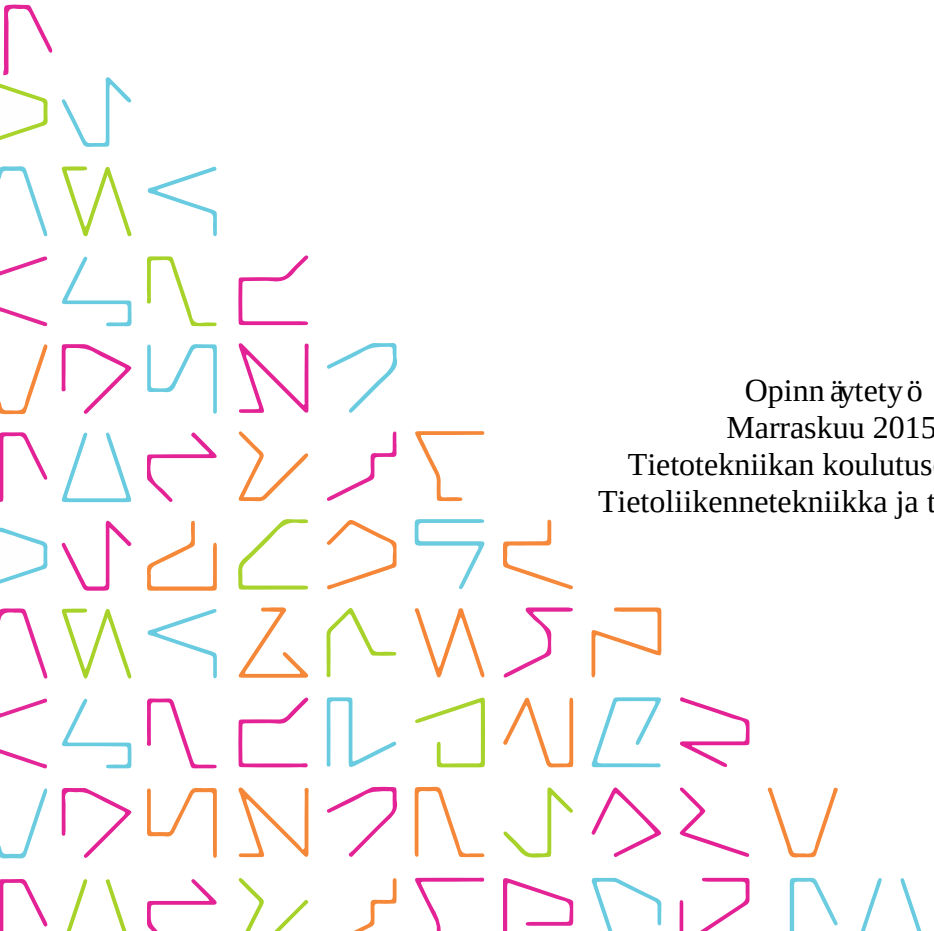
TAMPEREEN
AMMATTIKORKEAKOULU

PK-YRITYKSEN IT-INFRASTRUKTUURI PILVITOTEUTUKSENA

Teemu Konkola



Opinnäytetyö
Marraskuu 2015
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka ja tietoverkot

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka ja tietoverkot

KONKOLA, TEEMU
PK-yrityksen IT-infrastruktuuri pilvitoteutuksena

Opinnäytetyö 44 sivua
Marraskuu 2015

Tämä opinnäytetyö kuvaa IT-infrastruktuuriratkaisuja hypoteettiselle PK-yritykselle.

Työssä keskitytään luomaan tee-se-itse näkökulmasta katsottuna kustannustehokkaasti ja itsehallinteisesti IT-infran peruselementit, tiedostonjakokanavat, web-palvelut, sekä järkeistämään sisäinen ja ulkoinen viestintä.

Työn tavoitteena on tuoda uusia näkökulmia IT-infrastruktuurin rakentamiseen ja ylläpitoon, sekä oman malliratkaisun luonti käyttäen nykypäivän pilvipalvelumahdollisuuksia ja tekniikkaa.

Toteutukselle valittiin Amazon Web Services-pilvipalvelualusta Ubuntu Server 14.04 LTS EC2-palvelimien virtualisointiin ja ylläpitoon, soveltaen LEMP Stack-web kehitysalustaa, vsFTPd-tiedostonhallintaa, sekä iRedMail-sähköpostipalveluja.

Sisäisen viestinnän pääalustaksi valittiin järjestelmäriippumaton Slack-kommunikaatioalusta, joka toimii palveluiden keskittymänä, sekä joustavana integraatioalustana.

Asiasanat: it-infrastruktuuri pilvipalvelut aws palvelimet linux virtualisointi

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree programme in ICT Engineering
Telecommunications and Networks

KONKOLA, TEEMU
Cloud based IT Infrastructure for SMEs

Bachelor's thesis 44 pages
November 2015

This bachelor’s thesis describes IT infrastructure solutions of a hypothetical small and medium-sized enterprise.

The thesis focuses on creating a cost-effective and self-managed IT infrastructure in a do-it-yourself manner that includes file-sharing channels, web services, and rationalization of internal and external communications.

The thesis aims to bring new perspectives to the development, management and maintenance of an IT infrastructure as well as to create an example solution using today's cloud service opportunities and technology.

Amazon Web Services was chosen as the cloud platform for the virtualization and management of Ubuntu 14.04 LTS's EC2 servers. Virtualized Linux instances allow implementation of various highly customizable applications such as LEMP Stack for web services and development, vsFTPd for file management and iRedMail for email services.

Slack was chosen as the main communication cross-platform service to make internal communication more effective as well as serving as a highly customizable and flexible integration platform.

Key words: it infrastructure cloud aws servers linux virtualization

SISÄLLYS

ERITYISSANASTO tai LYHENTEET JA TERMIT (valitse jompikumpi)

AWS	Amazon Web Services
IaaS	Infrastructure as a Service, virtuaalinen konesali pilvessä
AMI	Amazon Machine Image, levykuva
EC2	Amazon Elastic Compute Cloud, virtuaalipalvelin
vCPU	Virtual Central Processing Unit, virtuaalinen prosessori
VPC	Virtual Private Cloud, yksityinen pilvi
EIP	Elastic IP, hallittava staattinen IP-osoite
Sudo	Ohjelma komentojen suorittamiseen pääkäyttäjänä
RSA	Julkisen avaimen salausalgoritmi
SSH	Secure Shell, tietoliikenteen salausprotokolla
SSL	Secure Sockets Layer, verkkoliikenteen salausprotokolla
TLS	Transport Layer Security, verkkoliikenteen salausprotokolla
HTTP	Hypertext Transfer Protocol, hypertekstin siirtoprotokolla
HTTPS	Hypertext Transfer Protocol Secure, HTTP-protokollan ja TLS/SSL-protokollan yhdistelmä
PHP	PHP: Hypertext Preprocessor, ohjelmointikieli
MySQL	Relaatiotietokantaohjelmisto
TCP	Transmission Control Protocol, tietoliikenneprotokolla yhteyksien luontiin verkkolaitteiden välillä
SFTP	Secure File Transfer Protocol, tiedonsiirtoprotokolla
vsFTPd	very secure File Transfer Protocol daemon, FTP-palvelin unix ympäristössä
FQDN	Fully Qualified Domain Name, domainin täysipitkä nimi
SMTP	Simple Mail Transfer Protocol, sähköpostinvälitysprotokolla
POP3	Post Office Protocol v.3, yksinkertainen sähköpostin hakemiseen tarkoitettu protokolla
IMAP	Internet Message Access Protocol, sähköpostien hakemiseen tarkoitettu protokolla
DNS	Domain Name System, nimipalvelujärjestelmä, joka muuttaa verkkotunnuksia IP-osoitteiksi
MX-Record	Mail Exchange Record, DNS-tietue sähköpostin ohjaamiseen
A-Record	DNS-tietue, joka ohjaa domainin palvelimen IP-osoitteeseen

1 JOHDANTO

Tämä opinnäytetyö kuvaa IT-infrastruktuuriratkaisuja hypoteettiselle PK-yritykselle. Työssä keskitytään luomaan tee-se-itse näkökulmassa kustannustehokkaasti ja itsehallinteisesti IT-infran peruselementit. Työn tavoitteena on luoda valmis kokonaisuus, joka kattaa yrityksen tai yhteisön tärkeimmät IT-palvelut eli sähköpostipalvelun, tietoturvallisen verkkotallennustilan, web-kehitysalustan ja sisäisen viestinnän työkalun, sekä mahdollisuuden integrointiin ja monipuoliseen toteutukseen.

Toimivan IT-infrastruktuurin pitäisi olla helposti hallittavissa, tietoturvallinen, kustannustehokas, käyttäjäystävällinen ja ennen kaikkea vakaa. Tätä määritelmää ajatellen työssä on keskitytty luomaan palvelut mahdollisimman yhtenäisesti Amazon Web Services alustalla, sekä muita pilvipalveluja hyödyntäen, liikaa hajautusta vältäen.

Kaikki palvelut on toteutettu erittäin kustomoitavia ja sovellettettavia ohjelmistoja käyttäen, antaen käyttäjälleen monipuoliset ja kilpailukykyiset työkalut nykyajan IT-maailmassa.

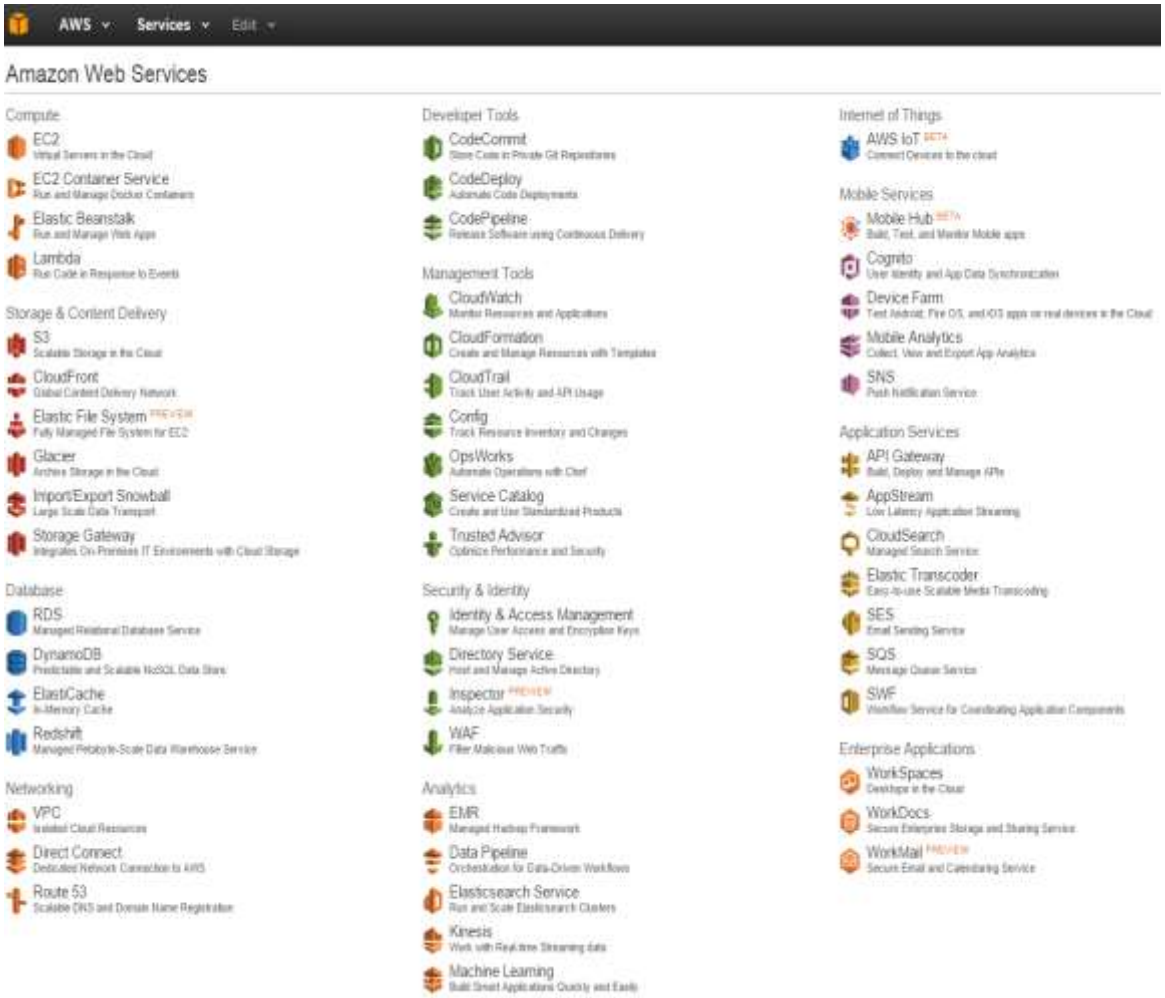
Työn runkona toimii Amazon Web Services monimutoinen pilvipalvelualusta, jonka avulla virtualisoidaan tarvittavat palvelimet ja palvelut. Palvelut toteutetaan Ubuntu Server 14.04 LTS EC2-instassien sisällä ja instasseja operoidaan PuTTy SSH-client ohjelmalla. Työssä kuvataan AWS alustan käyttöä ja hallintaa, sekä perehdytään perustietoturvaan palomuurisääntöjen ja julkisen avaimen salauksen myötä.

Työssä hyödynnetään LEMP Stack-palvelinkokonaisuutta web- ja vsFTPd-palvelinten rakentamiseen, sekä luodaan oma sähköpostipalvelin ja webmail-käyttöliittymä iRedMail-sähköpostiohjelmiston automatisoidun asennuspaketin avulla. Lopuksi työssä esitellään sisäisen viestinnän ohjelmisto Slack, joka toimii kokonaisuuden käyttäjärajapintana. Slack sisältää mahdollisuudet integroida ja liittää kaikki aikaisemmin luodut palvelut käyttäjätasolla yhteen.

2 AMAZON WEB SERVICES-PILVIPALVELUALUSTA

2.1 Käyttöliittymä ja instanssit

Amazon Web Services on maailman suurin maksullinen pilvipalvelualusta yksityisille kuluttajille, sekä yrityksille (Darrow 2015). AWS tarjoaa erittäin laajan valikoiman erilaisia pilvipalveluja (ks. Kuva 1). Käyttöönotto vaatii rekisteröitymisen palveluun, sekä luottokorttitietojen täyttämisen. Kirjautumisen jälkeen avautuu AWS Management Console, jota kautta pilvialustaa hallitaan.

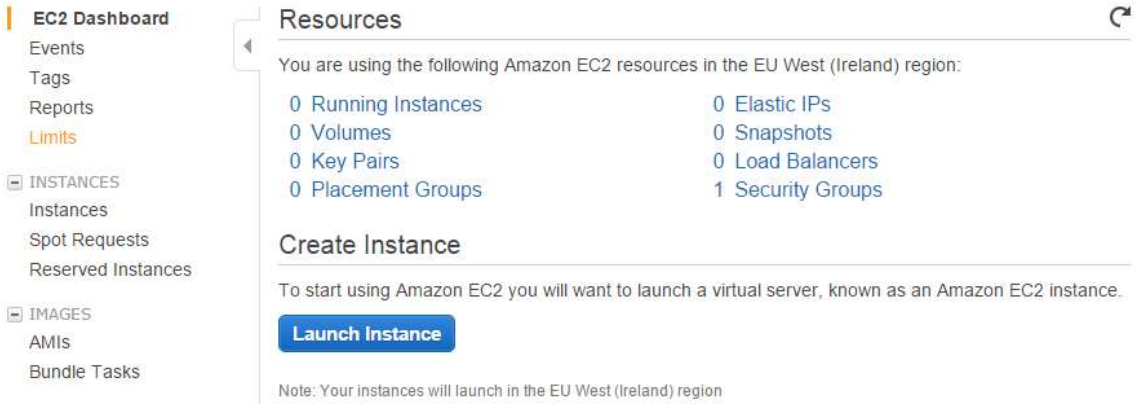


KUVA 1. Amazonin tarjoamat pilvipalvelut

2.2 EC2 instanssin luonti ja käyttöönotto

Amazon Elastic Compute Cloud (EC2) on osa AWS:n tarjoamaa IaaS alustaa. EC2-instanssit ovat virtuaalikoneita, joihin ladataan AMI-levykuvia (Amazon Machine Image). Amazon tarjoaa laajan valikoiman erilaisia AMI-levykuvia, useimmat Linux distribuutiot sekä Windows, että Unix-käyttöjärjestelmät löytyvät AWS-levykuvakirjastosta. (What Is Amazon EC2? 2015.)

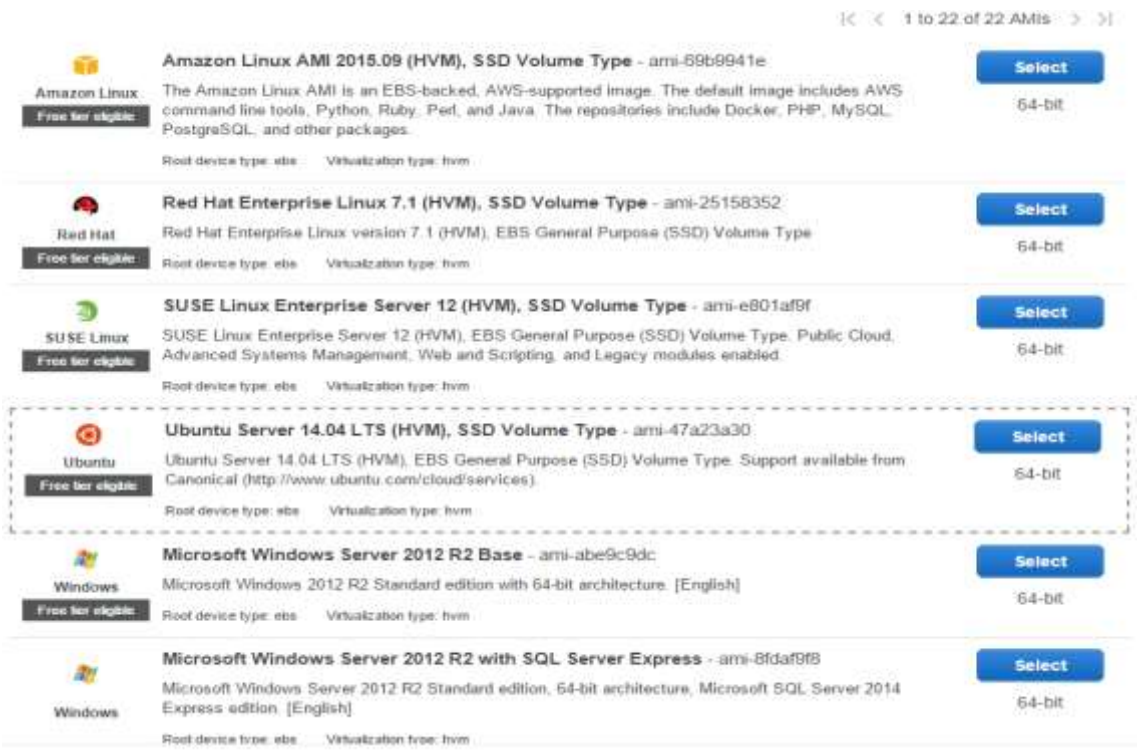
EC2-instanssin luonti on muutaman askeleen prosessi, ensiksi valitaan haluama pilvipalvelu (EC2) kuvan 1 palvelulistasta ja aloitetaan prosessi EC2 Dashboard-paneelin kautta, Launch Instance-painikkeella.



KUVA 2. EC2-hallintapaneelin oletusnäkymä

Seuraavaksi valitaan käyttöjärjestelmä eli AMI-levykuva ja instanssityyppi, tässä työssä käytettiin 64-bit Ubuntu Server 14.04 LTS AMI-levykuvaa, sekä ilmaista t2.micro tason virtuaalikokoonpanoa, joka sisältää alustavasti mm. 2.5 GHz Intel Xeon vCPU:n, 1 GB keskusmuistia ja 8 GB kovalevytilaa.

Instanssia luotaessa AWS tarjoaa monia kustomointimahdollisuuksia, kuten esimerkiksi instanssien määrän säätelyn, VPC-mahdollisuuden (Virtual Private Cloud), kovalevytilaa, monitorointipalvelun, palomuurisääntöjen muokkausta ja erinäisten hallintametodien yhdistämistä (AWS UserGuide EC2 2015). Työn instanssi luotiin oletusarvoja mukaillen.



KUVA 3. AMI-levykuvia listan äkym äss ä

Prosessin lopuksi n ähd ään yhteenveto instanssin asetuksista, sek ä valitaan avainparit (2.2.1 Avainparit ja Palomuuris ään öt), jonka j älkeen instanssi k äynnistyy (ks. Kuva 4).

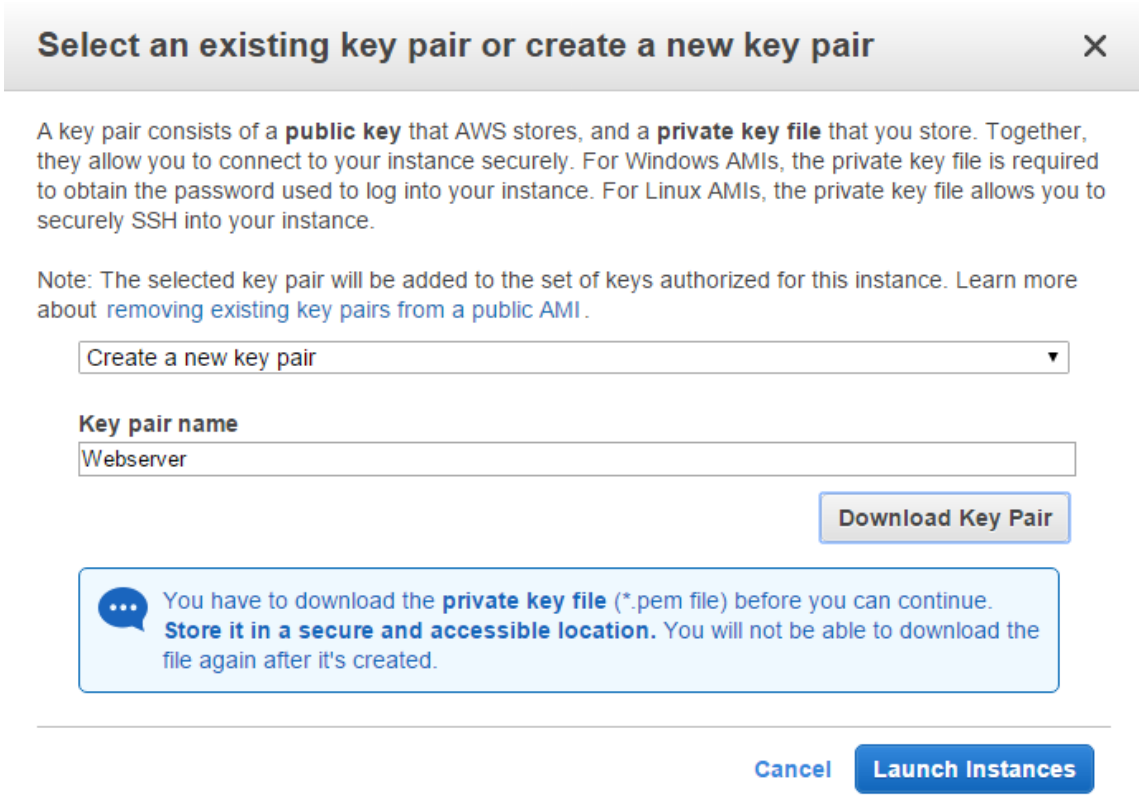
KUVA 4. K äynniss ä olevat instanssit

2.2.1 Avainparit ja palomuuris ään öt

Julkisen avaimen salaus on ep äsymmetrist ä salausta, jossa k äytettyj ä avaimia ei laskutoimitusten vaativuuden takia k äyt ännöss ä voi p ätell ä toisistaan. Niinp ä vain toinen avaimista tarvitsee pit ää yksityisen ä, kun taas toinen voidaan julkaista. (Wikipedia 2015). Julkisen avaimen salausalgoritmit esim. RSA, (Amazonilla 2048-bit SSH-2 RSA) ovat laajalti k äytetty ep äsymmetrisen salauksen muoto, mink ä seurauksena "ep äsymmetrist ä" ja "julkisen avaimen salausta" k äytet ään pitk älti synonyymien tavoin (Amazon EC2 Key Pairs 2015).

Amazon EC2 käyttää julkisen avaimen kryptausmenetelmää kirjautumisen suojana. Salausmenetelmä käyttää julkista avainta kryptatakseen dataa, kuten salasanan tässä tapauksessa (Amazon EC2 Key Pairs 2015).

Kirjautuakseen sisään palvelimelle on luotava avainpari (ks. Kuva 5). Avainparille määritellään nimi ja avaimen privaattiosa ladataan käyttäjän tietokoneelle fyysisenä tiedostona.



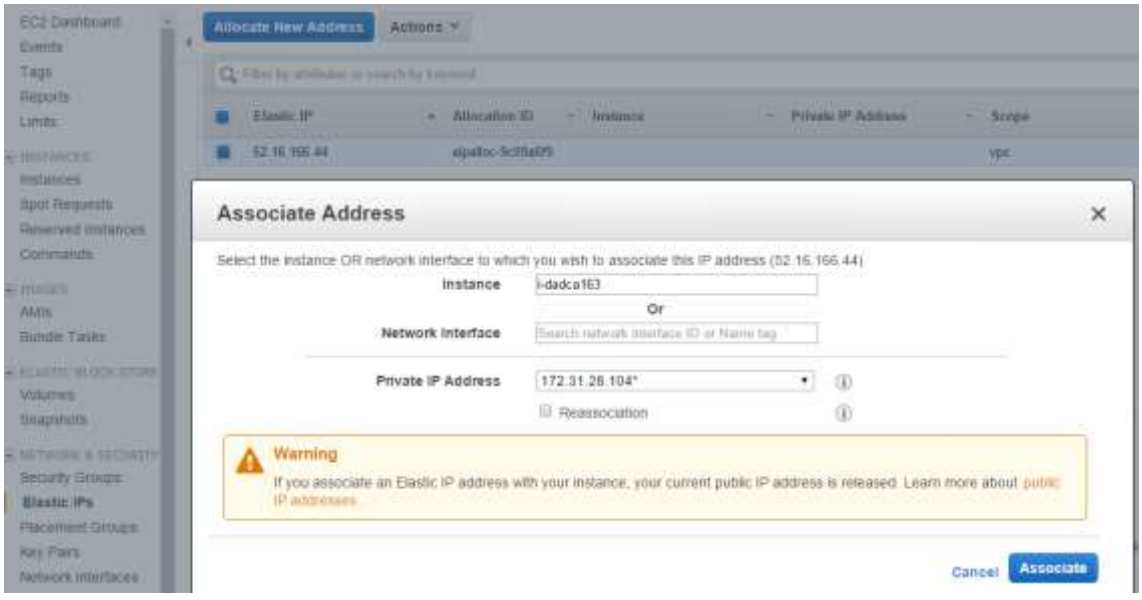
KUVA 5. Avainparin luonti instanssille

Jotta yhteyden muodostaminen onnistuu SSH-sovelluksella, täytyy AWS-hallintapaneelista määritellä EC2-instanssille palomuurisäännöt (Security Group), tarkemmin sanottuna SSH-portti nro. 22 täytyy avata. Myöhemmin myös portit 80 (HTTP), sekä 443 (HTTPS) täytyy avata web-palveluita varten. Kuvassa 6 näkyy aukaistut portit. Tietoturvan kannalta on hyvä asettaa oma IP-osoite source-kohtaan, tämä estää yhteyksien muodostamisen muista IP-osoitteista.

KUVA 6. Security Group – palomuuris ääntöjen muokkaus

2.2.2 Elastisen IP-osoitteen allokointi ja määritys

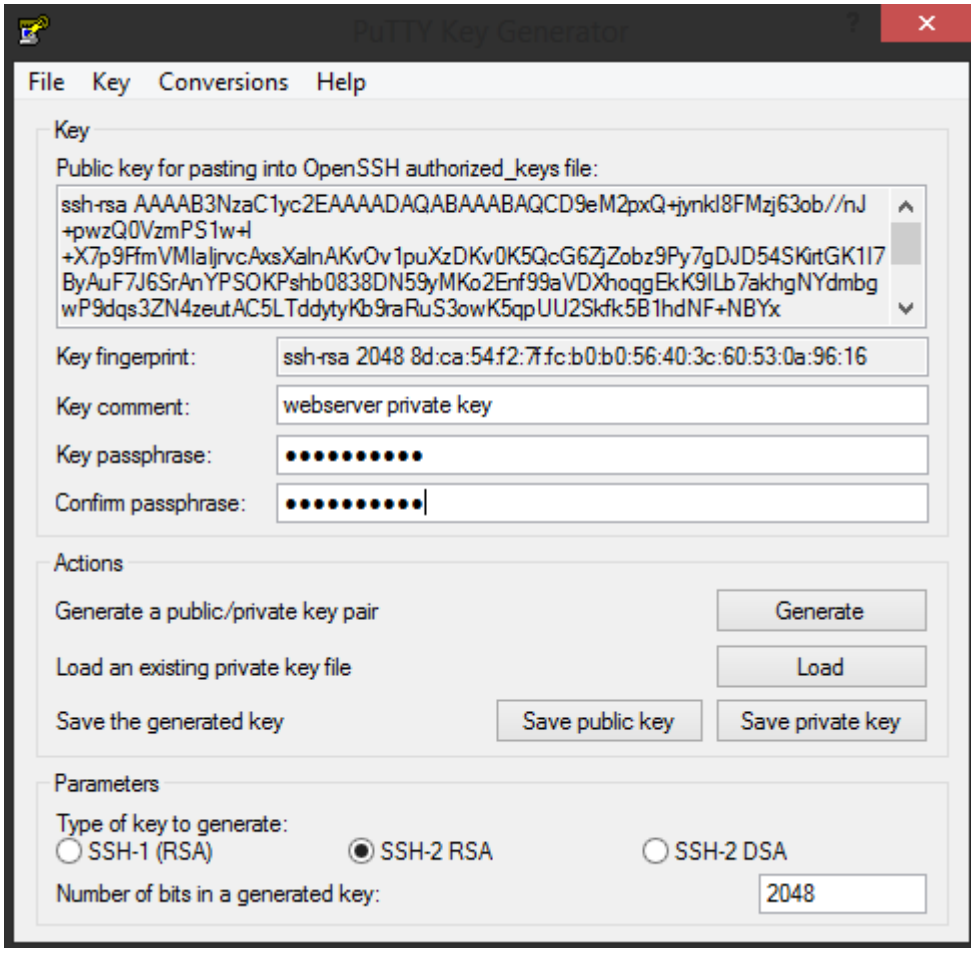
AWS tarjoaa mahdollisuuden varata omalle tunnukselle IP-osoitteita, joita voi jakaa tarpeen mukaan haluamille instansseille tai palveluille (Elastic IP Adresses 2015). AWS rohkaisee käyttäjiään varaamaan EIP:n (Elastic IP address) veloittamalla pienehkön summan, jos instanssit pyörivät alkuasetus IP:llä. EIP on vapaasti käytettävissä ja sen voi uudelleen määrittään tarpeen vaatiessa toiseen instanssiin tai palveluun (AWS UserGuide EIP 2015). Kuvassa 7 liitetään jo allokoitu EIP-osoite EC2-instanssiin. Julkista IP-osoitetta käytetään yhteyden muodostamiseen ja hallinnointiin.



KUVA 7. Elastisen IP:n liittäminen EC2-instanssiin.

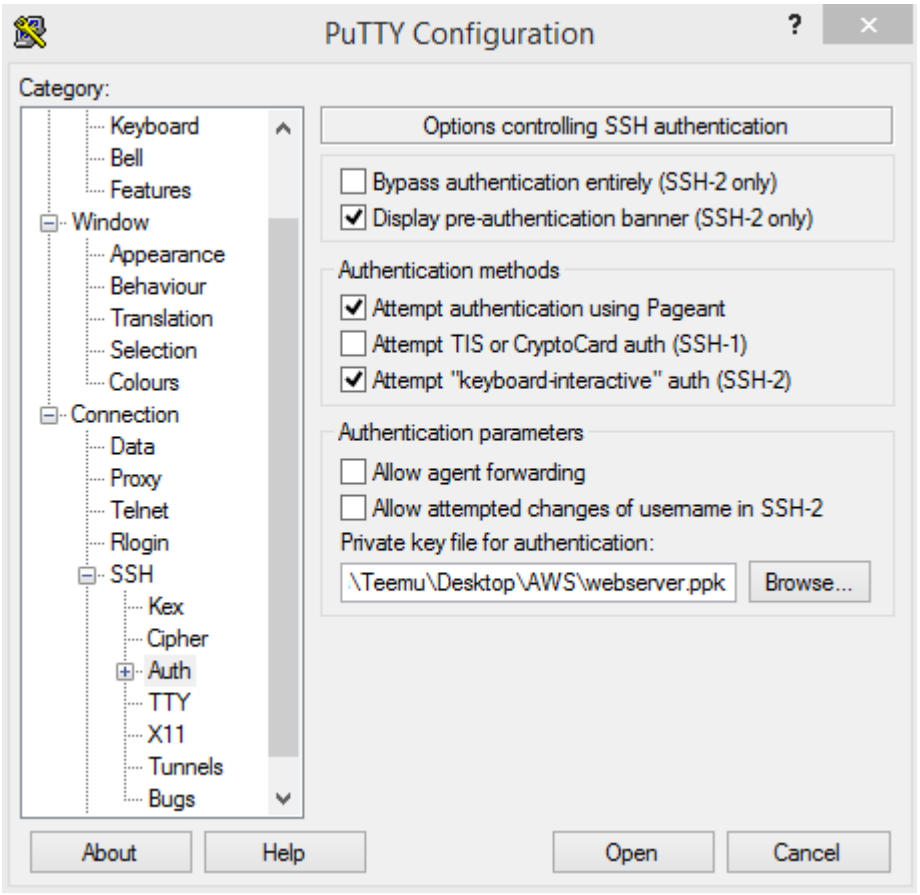
2.2.3 Yhteyden muodostaminen SSH:lla

Aikaisemmin web-palvelimelle asetetun avainparin .pem päätteinen tiedosto täytyy vielä prosessoida kuvan 8 mukaisesti. Esimerkissä käytetään PuTTy Key Generator-sovellusta, joka generoi .pem tiedostosta privaattiavaimen .ppk tiedostomuodossa (PuTTy Private Key file). Privaattiavain on muotoa SSH-2 RSA 2048 bit ja sille määritellään erikseen oma salasana, jota käytetään kirjautumisen yhteydessä.



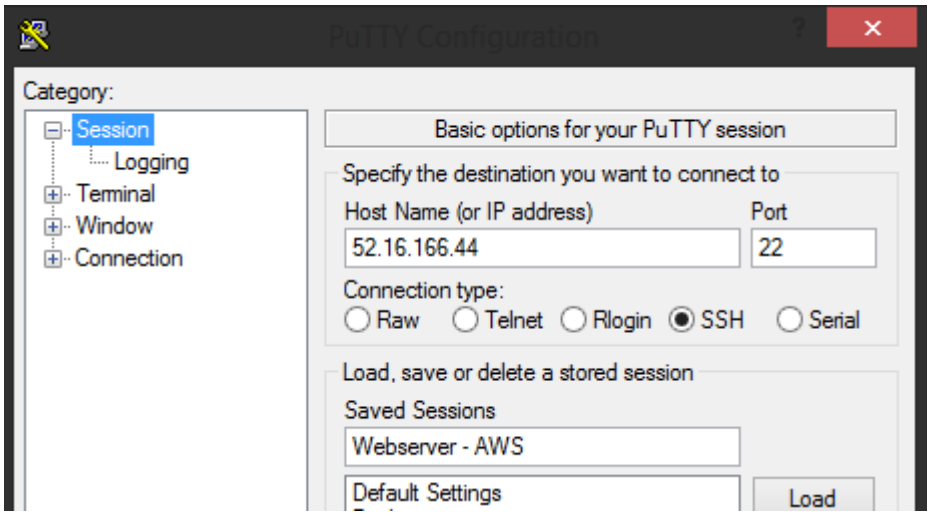
KUVA 8. PuTTy Key Generator

Yhteyden muodostamiseksi avataan PuTTy:sta uusi Sessio ja syötetään instanssin julkinen IP-osoite PuTTy:n Host Name-kenttään, sekä valitaan Authentication välilehdeltä generoitu privaattiavain (.ppk) autentikointia varten (ks. Kuva 9).



KUVA 9. PuTTy privaattiavaimen valitseminen autentikointia varten

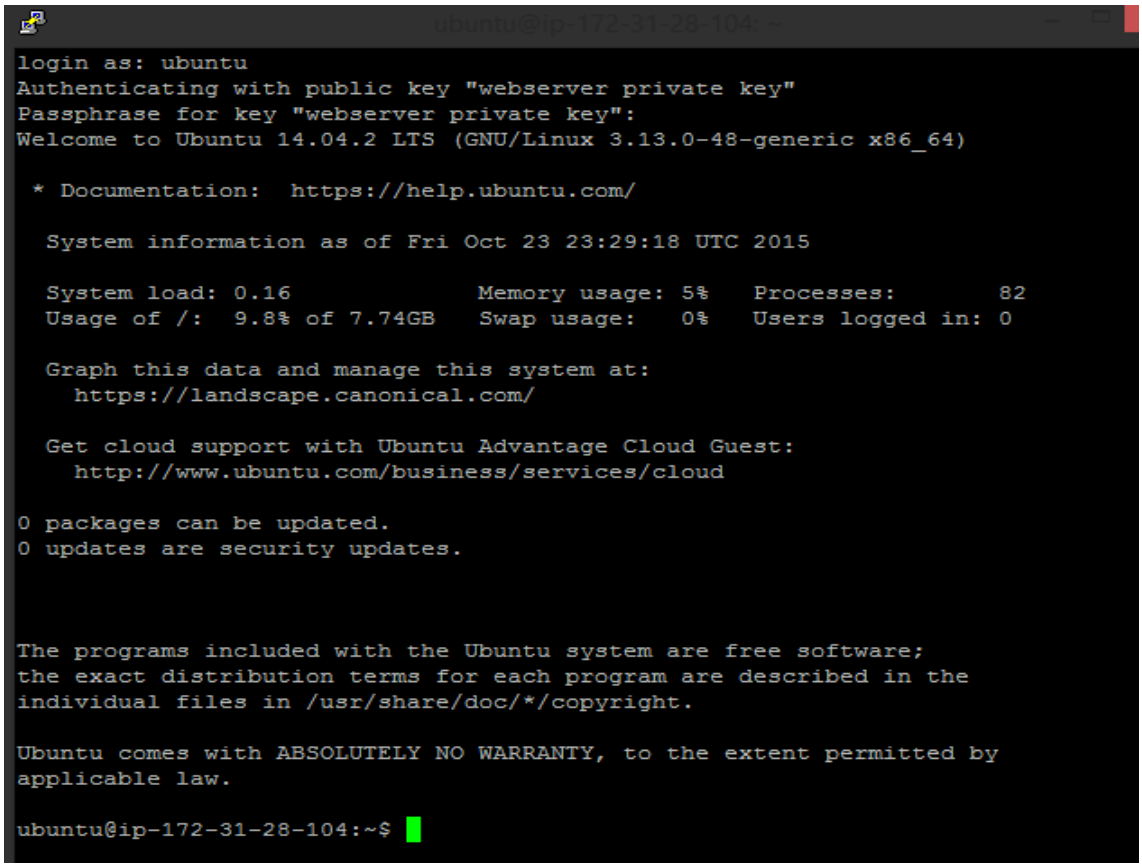
Kuvassa 10 näkyy PuTTy Sessionin alkuparametrit, EC2-instanssin julkinen IP, sekä SSH portti 22, joka aukaistiin aikaisemmin.



KUVA 10. PuTTy Sessiokonfiguraatio

Yhteyttä muodostaessa ensimmäistä kertaa käytetään kirjautumistunnuksena EC2-ubuntu AMI-instanssin oletuskirjautumisnimeä **ubuntu**. EC2-instanssi suorittaa autentikoinnin julkisen- ja privaattiavaimen salausmetodilla, sekä kysyy

privaattiavaimelle asetettua salasanaa. Aloitusruudussa näkyy Linuxille tyypilliseen tapaan käyttöjärjestelmän versio, päivitys- ja käyttäjätietoja sekä kuormitus- ja prosessitietoja.



KUVA 11. EC2-instanssin kirjautumisnäkymä

2.3 Perustietoturva ja käyttöoikeudet

2.3.1 Uuden käyttäjän luominen ja käyttöoikeuksien lisääminen

Perustietoturvan kannalta on oleellista luoda uusi käyttäjätunnus ja määrittää tälle SSH-kirjautumisoikeudet, sekä poistaa oletusarvoinen käyttäjätunnus. Uusi tunnus luodaan komennolla **sudo adduser käyttäjänimi**, jonka jälkeen tunnukselle määritellään halutut oikeudet. Työssä uudelle käyttäjälle ”newbie” määritellään sudo-oikeudet sudoer-tiedostossa. Tiedostoon pääsee käsiksi parilla eri tapaa, yksi tapa on vaihtaa root-käyttäjäksi **su –i** komennolla ja käyttää komentoa **visudo**.

```
ubuntu@ip-172-31-26-24:~$ sudo adduser newbie
ubuntu@ip-172-31-26-24:~$ sudo -i
root@ip-172-31-26-24:~# visudo
```

```
ubuntu@ip-172-31-28-104:~$ sudo adduser newuser
Adding user `newuser' ...
Adding new group `newuser' (1002) ...
Adding new user `newuser' (1002) with group `newuser' ...
Creating home directory `/home/newuser' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for newuser
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
ubuntu@ip-172-31-28-104:~$
```

KUVA 12. Uuden käyttäjätunnuksen luominen

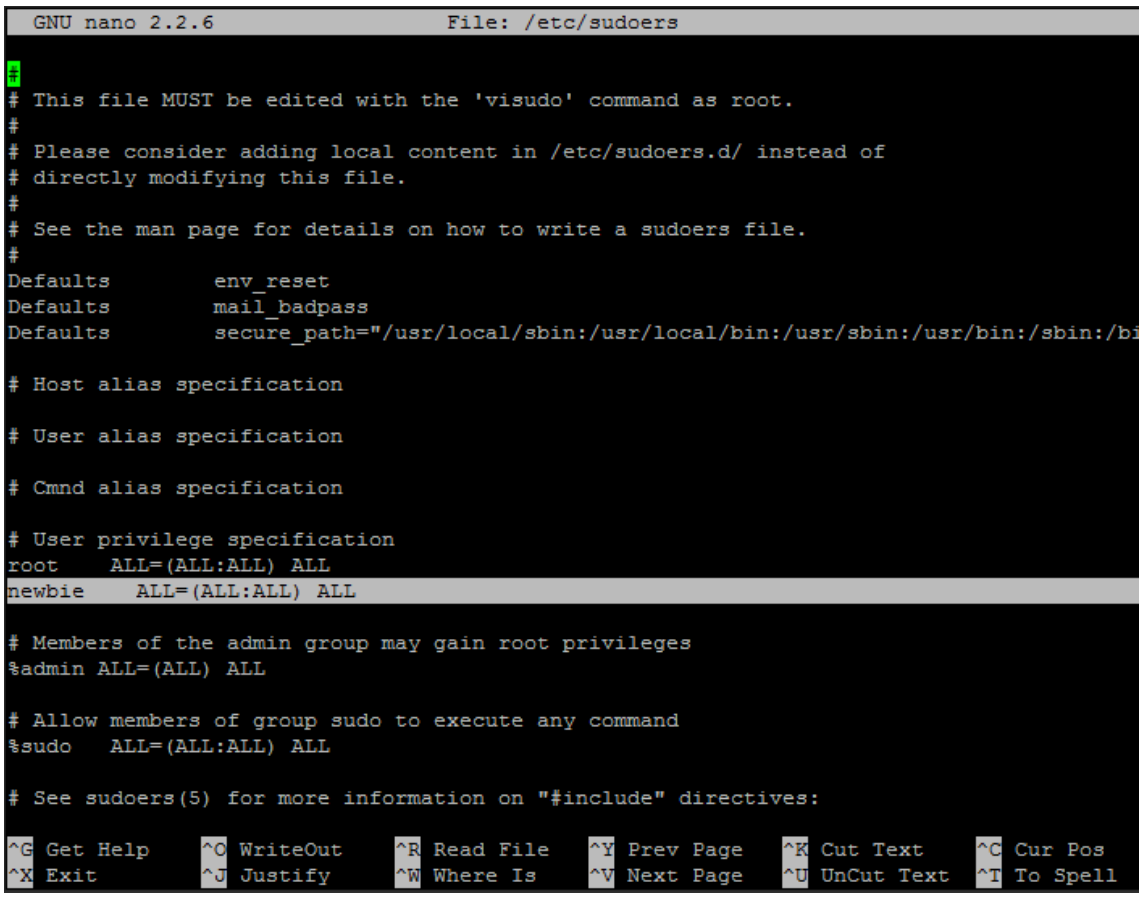
Toinen tapa on muokata tiedostoa suoraan **sudo nano /etc/sudoers** komennolla.

```
ubuntu@ip-172-31-26-24:~$ sudo nano /etc/sudoers
```

Kuvassa 13 sudoers-tiedostoon lisätään rivi **# User privilege specification** kohdan alle, joka käytännössä antaa newbie-käyttäjätunnukselle sudo-oikeudet.

root ALL=(ALL:ALL) ALL

newbie ALL=(ALL:ALL) ALL



KUVA 13. Käyttöoikeuksien lisääminen sudoers-tiedostossa

2.3.2 SSH-yhteyden salliminen uudelle käyttäjälle

SSH-kirjautumisen sallimiseksi uudelle käyttäjälle tarvitsee luoda julkiselle avaimelle oma tiedosto käyttäjän kotihakemistoon. Käyttöoikeuksien lisäämisen jälkeen vaihdetaan käyttäjää (newbie) ja luodaan .ssh niminen tiedostopolku, sekä muutetaan polun käyttöoikeudet siten, että vain newbie-käyttäjä saa oikeudet avata, lukea ja kirjoittaa (Read, Write, Open) kyseiseen polkuun.

```
ubuntu@ip-172-31-26-24:~$ su newbie
newbie@ip-172-31-26-24:~$ cd
newbie@ip-172-31-26-24:~$ mkdir .ssh
newbie@ip-172-31-26-24:~$ chmod 700 .ssh
```

Luodaan uudelle käyttäjälle (newbie) tiedosto julkiselle avaimelle (authorized_keys) .ssh polkuun **touch**-komennolla, sekä määritellään käyttäjäkohtaiset luku- ja kirjoitusoikeudet.

```
newbie@ip-172-31-26-24:~$ touch .ssh/authorized_keys
newbie@ip-172-31-26-24:~$ chmod 600 .ssh/authorized_keys
```

Julkinen avain löytyy ubuntu-käyttäjän hakemistosta .ssh/authorized_keys ja sen sisältö kopioidaan newbie-käyttäjän vastaavaan tiedostoon.

```
ubuntu@ip-172-31-28-104:~$ sudo vim .ssh/authorized_keys
newbie@ip-172-31-26-24:~$ nano .ssh/authorized_keys
```

Näiden komentojen jälkeen newbie-käyttäjätunnuksella pystyy kirjautumaan sisään SSH:lla, sekä toimimaan sudo-käyttäjänä. Oletuskäyttäjää ubuntua ei enää tarvita, joten se voidaan poistaa.

```
newbie@ip-172-31-28-104:~$ sudo userdel –r ubuntu
```

Palvelimelle voi myös haluttaessa asettaa uuden isäntänimen (hostname), esimerkiksi Webserver. Muutokset tehdään tiedostoihin /etc/hostname ja /etc/hosts. Muutokset tulevat voimaan palvelimen uudelleenkäynnistyksen jälkeen.

```
newbie@ip-172-31-28-104:~$ sudo nano /etc/hostname
newbie@ip-172-31-28-104:~$ sudo nano /etc/hosts
newbie@ip-172-31-28-104:~$ sudo nano reboot
newbie@webserver:~$
```

3 WEB-PALVELINSOVELLUKSET

Tässä kappaleessa tarkastellaan web-palvelimen sovelluksia kokonaisuutena, Nginx-pohjaista LEMP-stackia käytetään kokonaisuuden runkona ja siihen sovelletaan web-hallinteinen MySQL-tietokanta (phpMyAdmin), sekä vsFTPd-tiedostojen tallennuspalvelin. Web-palvelin ja sen liitännäiset eivät itsessään vaadi domain-osoitetta toimiakseen, mutta email-palvelin taas vaatii, joten työlle varattiin ilmainen domain-osoite ”newbiex.tk” freenom-sivustolta ja luotiin A-tietue DNS-tietoihin web-palvelinta varten. Myöhemmin DNS-tietoihin tullaan tekemään lisäyksiä email-palvelimelle (ks. Kuva 29 DNS-tietueen lisääminen email-palvelimelle).

3.1 LEMP-stack web-palvelinratkaisu

Web-palvelinratkaisuksi työhön valittiin LEMP-stack (Linux, NGINX, MySQL, PHP). LEMP on ryhmä avoimen lähdekoodin ohjelmistoja, jotka kokonaisuutena rakentavat tehokkaan ja kevyen web-palvelimen. LEMP koostuu Linuxista, NGINX web-palvelimesta, MySQL tietokantapalvelimesta, sekä PHP:sta (NGINX Wiki 2015).

Muita varteenotettavia web-palvelinratkaisuja ja tekniikoita ovat esimerkiksi javascript-pohjainen MEAN-stack (MongoDB, ExpressJS, AngularJS, Node.js), Microsoft IIS (Internet Information Service), sekä perinteisemmät LAMP/WAMP-stacks (Linux tai Windows, Apache, MySQL, PHP) (Richardson 2013).

3.1.1 MySQL-palvelin

MySQL on tehokas avoimeen lähdekoodiin perustuva relaatiotietokantaohjelmisto, joka käsittelee SQL-tietokantapyyntöjä (Structured Query Language) nopeasti ja tehokkaasti (MySQL Manual 2015).

LEMP-stackin kokoaminen aloitetaan MySQL-palvelimen asennuksella. Palvelimen asennuksen yhteydessä ohjelma pyytää asettamaan MySQL root-käyttäjälle salasanan,

jonka jälkeen ohjelma asentaa ja konfiguroi palvelimen loppuun. Root-käyttäjän salasana on tarvittaessa asetettavissa myös myöhemmin MySQL shellin kautta.

```
newbie@webserver:~$ sudo apt-get install mysql-server php5-
```

Asennuksen jälkeen luodaan MySQL datahakemistot, alustetaan järjestelmän taulukkorakenne, luodaan järjestelmänvalvoja-tili, sekä aktivoidaan tietokanta.

```
newbie@webserver:~$ sudo mysql_install_db
```

Viimeistellään asennus poistamalla käytöstä kuvan 14 mukaiset moduulit, anonymous users, root login, sekä test database. Nämä oletusmoduulit on tarkoitettu lähinnä testikäyttöä varten ja poistamalla moduulit saadaan palvelimesta hivenen turvallisempi.

```
newbie@webserver:~$ sudo /usr/bin/mysql_secure_installation
```

```
You already have a root password set, so you can safely answer 'n'.

Change the root password? [Y/n] n
 ... skipping.

By default, a MySQL installation has an anonymous user, allowing anyone
to log into MySQL without having to have a user account created for
them.  This is intended only for testing, and to make the installation
go a bit smoother.  You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] y
 ... Success!

Normally, root should only be allowed to connect from 'localhost'.  This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] y
 ... Success!

By default, MySQL comes with a database named 'test' that anyone can
access.  This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] y
 - Dropping test database...
ERROR 1008 (HY000) at line 1: Can't drop database 'test'; database doesn't exist
 ... Failed!  Not critical, keep moving...
 - Removing privileges on test database...
 ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] y
 ... Success!

Cleaning up...



All done!  If you've completed all of the above steps, your MySQL
installation should now be secure.

Thanks for using MySQL!
```

KUVA 14. MySQL asennuksen viimeistely

3.1.2 NGINX-web palvelin

NGINX (Engine-x) on ilmainen avoimen lähdekoodin HTTP-web palvelin, joka keskittyy suorituskykyyn ja vähäiseen muistin käyttöön. NGINX voi toimia myös käänteisproxyna HTTP, HTTPS, SMTP, POP3, sekä IMAP protokollille. (NGINX Wiki 2015.)

NGINX:n on arvioitu olevan kolmanneksi yleisin web-palvelin ja kilpailee Apachen, sekä Microsoftin IIS-palvelimen (Internet Information Services) kanssa. NGINX:n kilpailukyky perustuu vähäiseen resurssitarpeeseen, sekä erinomaiseen skaalautuvuuteen. (NGINX Wiki 2015.)

Asennetaan NGINX, sekä käynnistetään palvelin. Palvelimen toimivuus voidaan tarkistaa syöttämällä selaimen osoiteriville EC2-palvelimen julkinen IP-osoite. Kuvassa 15 on kuvattu onnistunut asennus.

```
newbie@webserver:~$ sudo apt-get install nginx
newbie@webserver:~$ sudo service nginx start
```

NGINX-palvelin tottelee yksiselitteisiä hallintakäskyjä.

```
newbie@webserver:~$ sudo service nginx start
newbie@webserver:~$ sudo service nginx stop
newbie@webserver:~$ sudo service nginx restart
```

NGINX-palvelimen pitäisi käynnistää itsensä oletusarvoisesti aina EC2-instanssin käynnistyttyä. Tämä voidaan vielä varmentaa seuraavalla komennolla.

```
newbie@ newbie@webserver:~$ sudo update-rc.d nginx defaults
```

KUVA 15. NGINX asennuksen tarkistus

3.2 PHP5-asennus

PHP (PHP: Hypertext Preprocessor) on lisenssivapaa avoimen lähdekoodiin perustuva yleishyödyllinen ja erittäin tunnettu skriptikieli, joka on pääsääntöisesti tarkoitettu Web-sovelluskehitykseen (PHP manual 2015). PHP-skriptit suoritetaan suoraan palvelimella, kieli tarjoaa erinomaisia web-kehitysmahdollisuuksia keskittyen back-end tekniikkaan. (NTC Hosting PHP5 2015).

3.2.1 PHP-FPM asennus

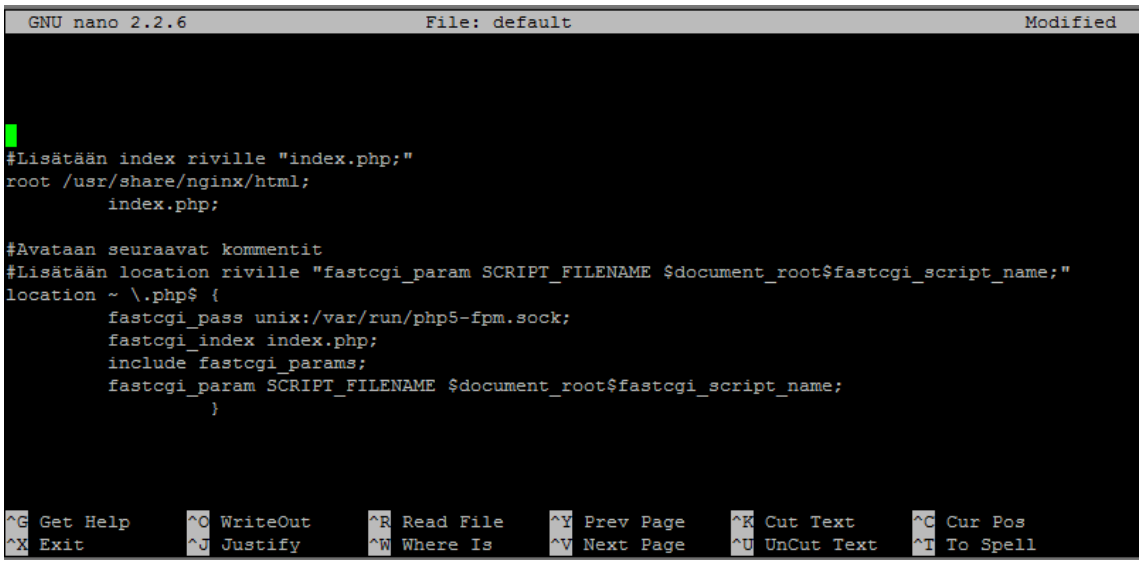
Noudetaan ja asennetaan PHP5-fpm, sekä muutetaan sen sisältämän php.ini tiedoston cgi.fix_pathinfo=1 arvoa nollaksi, tämä sulkee oletuskonfiguraation tietoturva-aukon. Lopuksi käynnistetään PHP-palvelin uudelleen.

```
newbie@ip-172-31-26-24:~$ sudo apt-get install php5-fpm
newbie@ip-172-31-26-24:~$ sudo nano /etc/php5/fpm/php.ini
cgi.fix_pathinfo=0;
newbie@ip-172-31-26-24:~$ sudo service php5-fpm restart
```

3.3 PHP:n soveltaminen NGINX:ssa

Valjastetaan PHP-fpm NGINX:n käyttöön konfiguroimalla default-tiedostoa kuvan 16 mukaisesti /nginx/sites-available/default.

```
newbie@webserver:~$ sudo nano /etc/nginx/sites-available/default
```

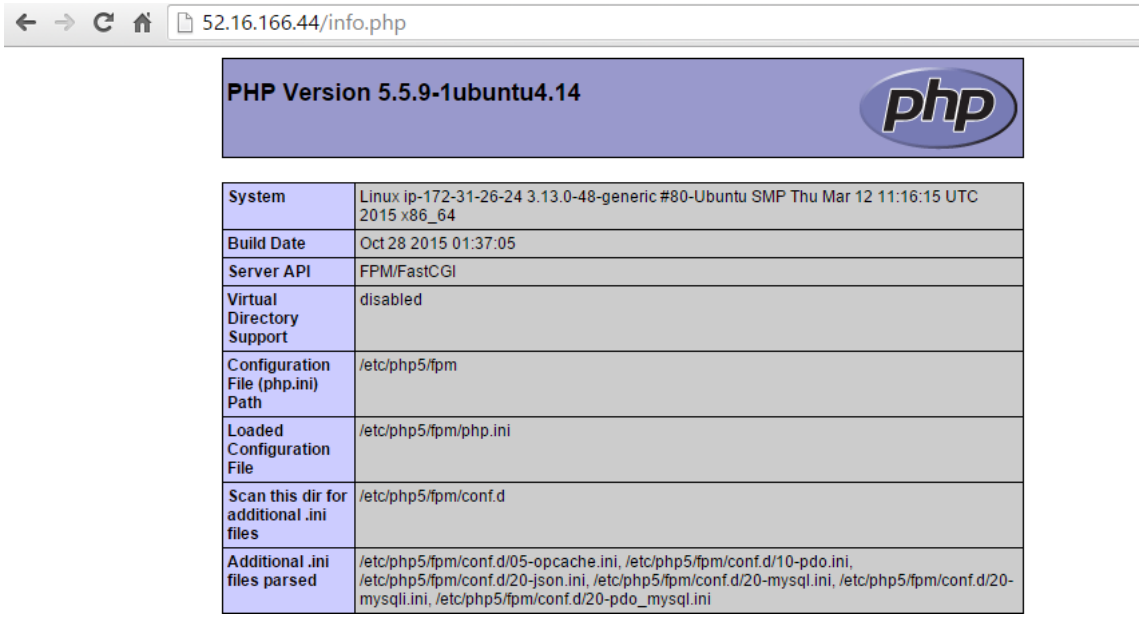


KUVA 16. PHP:n valmis konfiguraatio

PHP:n toimivuutta voidaan testata luomalla info.php tiedosto /usr/share/nginx/html/ polkuun lisäen tiedostoon phpinfo(); funktion. Funktio tulostaa laajan tietokerayksen web-palvelimen PHP-asetuksista ja tätä näkymää voi hyvin hyödyntää esimerkiksi viankorjauksessa (PHP manual 2015). Kuvassa 17 testataan palvelun toimivuus syöttämällä selaimeen omadomain-tai-julkinen-ip/info.php (tässä tapauksessa julkinen ip 52.16.166.44/info.php).

```
newbie@webserver:~$ sudo nano /usr/share/nginx/html/info.php
```

```
<?php
phpinfo();
?>
```



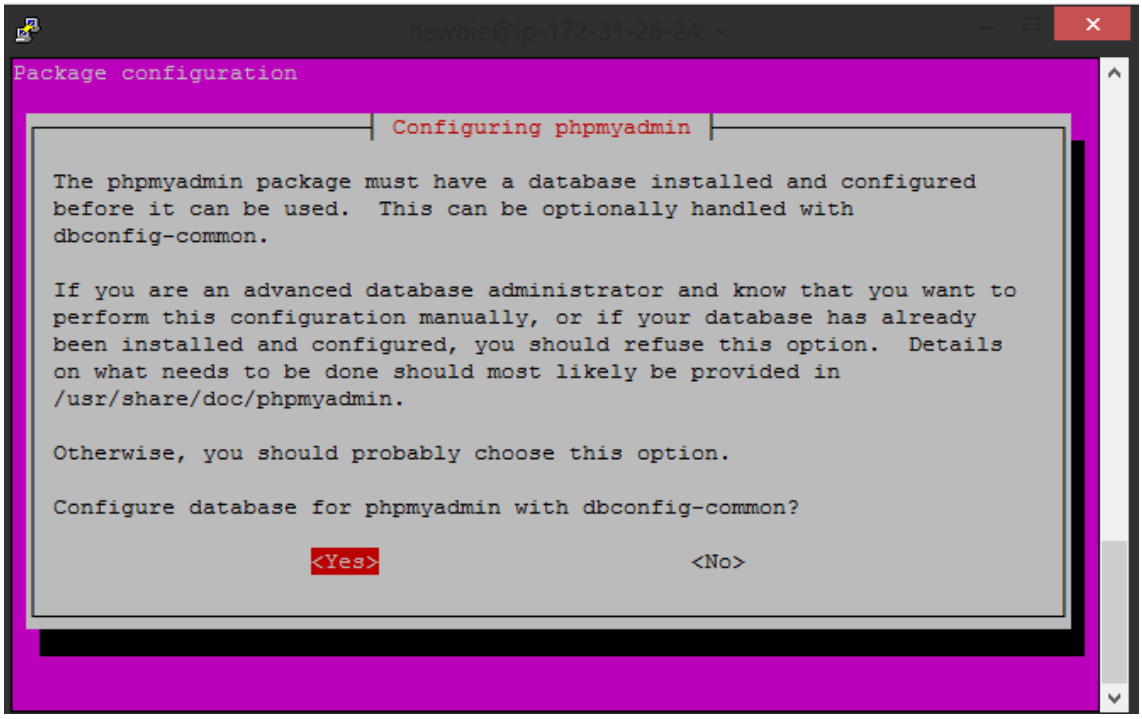
KUVA 17. php.info tiedoston tarkastelu selaimen äkymässä

3.3.1 phpMyAdmin asennus

PhpMyAdmin on ilmainen työkalu MySQL-tietokannan web-pohjaiseen hallintaan. Työkalun pääfunktiot ovat MySQL-tietokantojen hallinta, selaus ja varmuuskopiointi GUI:n kautta, phpMyAdmin tarjoaa myös mahdollisuuden käyttää perinteisiä SQL-lauseita. (phpMyAdmin 2015.)

Asennetaan phpMyAdmin oletusarvoisesti dbconfig-common-konfiguraatiolla (ks. Kuva 18). Prosessissa syötetään MySQL-palvelimen asennuksen yhteydessä määritelty pääkäyttäjän salasana, sekä määritellään erikseen phpMyAdmin-sovellukselle salasana, jota käytetään kirjautuessa palveluun selaimen kautta.

```
newbie@webserver:~$ sudo apt-get install phpmyadmin
```



KUVA 18. phpMyAdmin asennusn äkym ä dbconfig-common

Asennusprosessi tarjoaa myös kahden oletuspalvelimen automaattista konfigurointia (Apache tai lighthttpd), ohitetaan valinta painamalla **tab** ja **ok** (ks. Kuva 19).

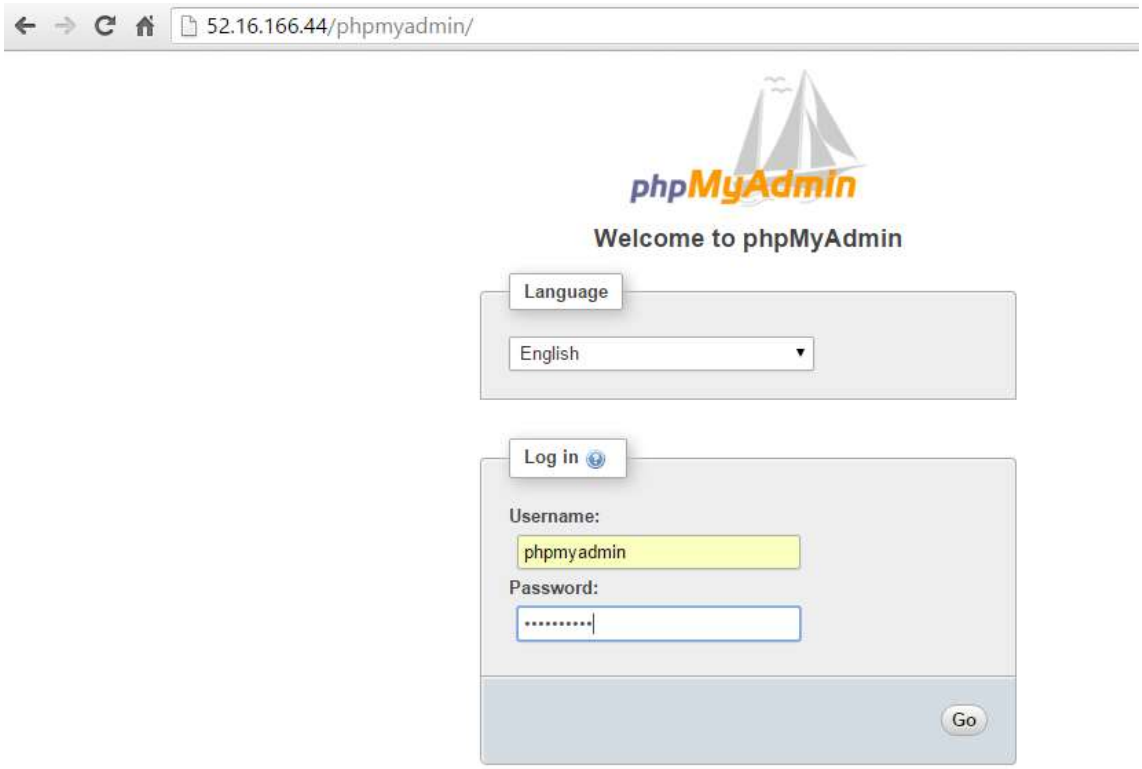
KUVA 19. phpMyAdmin oletuspalvelinkonfiguraation ohittaminen

3.3.2 phpMyAdmin konfigurointi

Asennuksen jälkeen luodaan symbolinen linkki phpMyAdmin:n ja NGINX -palvelimen tiedostopolun välille, sekä käynnistetään NGINX-palvelin uudelleen.

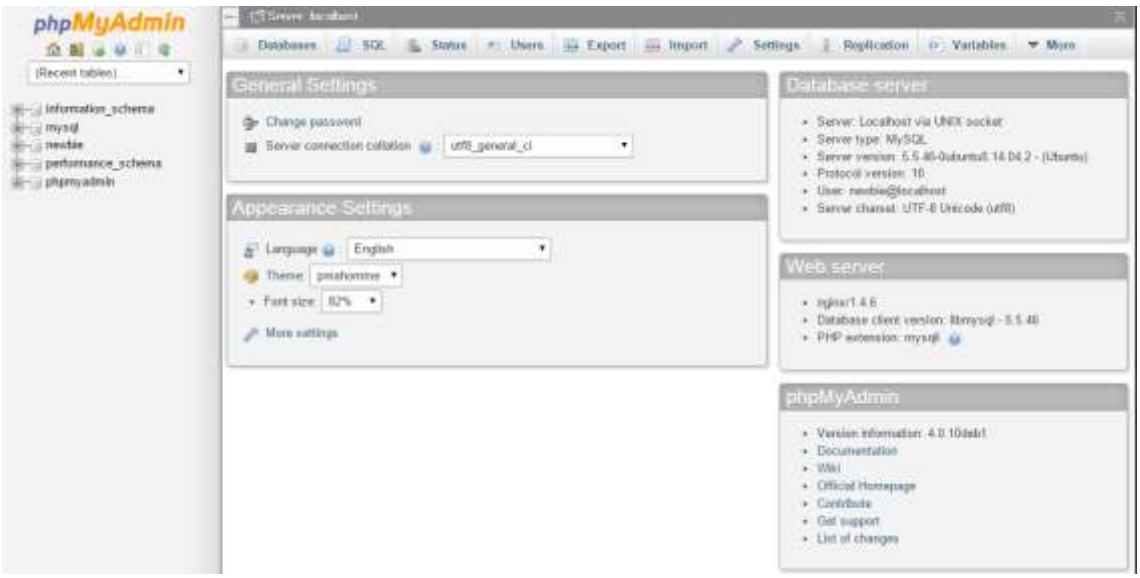
```
newbie@webserver:~$ sudo ln -s /usr/share/phpmyadmin/
/usr/share/nginx/html

newbie@webserver:~$ sudo service nginx restart
```

Itse sovellusta käytetään selaimen kautta ja siihen päästään käsiksi syöttämällä selaimen osoiteriville **xxx.xxx.xxx.xxx/phpmyadmin** (julkinen IP-osoite) tai **omadomain/phpmyadmin**. Palveluun kirjaudutaan admin- tai root-käyttäjätunnuksella phpmyadmin ja käytetään asennuksen yhteydessä määritelty ä salasanaa (ks. Kuva 20).



KUVA 20. phpMyAdmin kirjautumisnäkymä selaimessa

Kirjautumisen jälkeen työkalu on toimintakykyinen ja vapaasti sovellettavissa omiin käyttötarpeisiin. Kuvassa 21 on phpMyAdmin oletusnäkymä.



KUVA 21. phpMyAdmin hallintapaneeli

3.4 vsFTPd-tiedostovarastointi

VsFTPd-palvelin (very secure File Transfer Protocol daemon) on turvallinen tiedostonjako- ja hallintapalvelin (vsftpd.beasts 2009). Tarjolla on myös useita vaihtoehtoja tiedostonvarastoinnille pilvipalvelumarkkinoilla, esimerkiksi Amazon S3, Google Drive, Microsoft OneDrive tai Dropbox. Työssä kuitenkin pyritään toteuttamaan infran runko tee-se-itse mielessä juuri-tasolla ja välttämään liikaa hajautusta, sekä kustannuksia, joten vsFTPd-palvelimen pystyttäminen EC2-instanssiin on ratkaisu tiedostojen tallennukseen ja siirtoon.

3.4.1 vsFTPd:n asennus

Asennetaan vsFTpd ja muutetaan sen konfigia polussa **/etc/vsftpd.conf**, siten että **anonymoys_enable=YES** arvo muutetaan arvoksi **NO**, tämä muutos estää tuntemattomien käyttäjien pääsyn palvelimen tiedostoihin. Tämä on muutos on laajalti oletusarvoinen, mutta sen olemassaolo on hyvä tarkistaa. Varmistetaan myös, että **local_enable** ja **write_enable** arvot ovat **YES** ja tarvittaessa poistetaan **#**-kommenttimerkki näiden edestä, tämä takaa että käyttäjät saavat kirjoitusoikeudet hakemistoon.

```
newbie@webserver:~$ sudo apt-get install vsftpd
newbie@webserver:~$ sudo nano /etc/vsftpd.conf

# Allow anonymous FTP? (Disabled by default)
anonymous_enable=NO

# Uncomment this to allow local users to log in.
local_enable=YES

# Uncomment this to enable any form of FTP write command.
write_enable=YES
```

Poistetaan kommentointi **chroot_local_user=YES** rivilt ä, t ämä est ää paikallisen k äytt äj än p ääsyn muualle kuin omaan kotihakemistoon (root). Lopuksi tallennetaan muutokset ja suljetaan tiedosto.

```
chroot_local_user=YES
```

Luodaan vsFTPd:lle uusi käyttäjä ”ftpuser” ja muutetaan uuden k äytt äj än kotihakemiston omistajuus root-k äytt äj älle, sek ä luodaan ftpuser:n kotihakemiston sis ään erillinen hakemisto **files** ja asetetaan hakemiston omistajuus ftpuser:lle. Lopuksi k äynnistet ään vsFTPd-palvelin uudelleen.

```
newbie@webserver:~$ sudo adduser ftpuser
newbie@webserver:~$ sudo chown root:root /home/ftpuser
newbie@webserver:~$ sudo mkdir /home/ftpuser/files
newbie@webserver:~$ sudo chown ftpuser:ftpuser /home/ftpuser/files
```

3.4.2 SSL-sertifikaatin luominen vsFTPd:lle

Tietoturvan lis äämiseksi on syyt ä luoda vsFTPd:lle SSL sertifikaatti, joka salaa yhteyden selaimen ja palvelimen v älill ä (HowtoForge 2015). Asennetaan **openssh** ja luodaan vuoden voimassaoleva sertifikaatti.

```
newbie@webserver:~$ sudo apt-get install openssl
```

```
newbie@webserver:~$ sudo openssl req -x509 -nodes -days 365 -newkey
rsa:1024 -keyout /etc/ssl/private/vsftpd.pem -out
/etc/ssl/private/vsftpd.pem
```

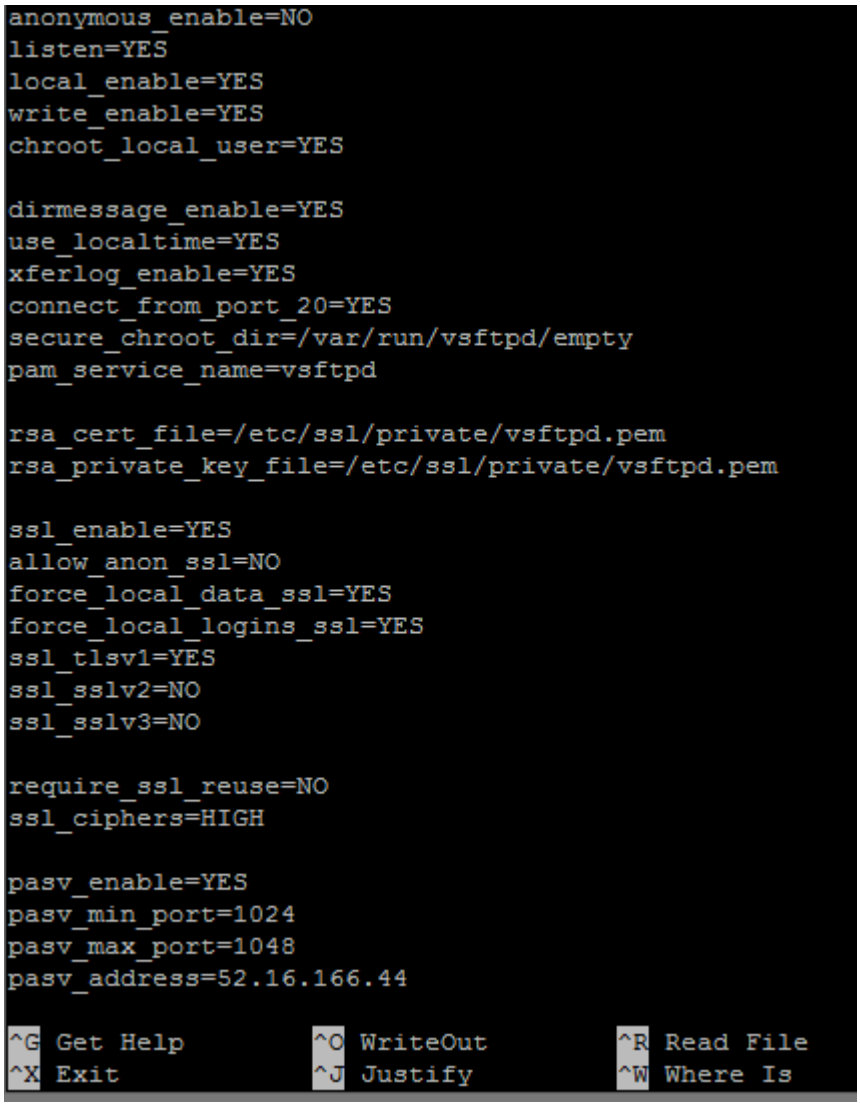
Konfiguroidaan SSL-tiedot vsFTPd:n konfigissa (/etc/vsftpd.conf), sekä osoitetaan avainparit kuvan 22. mukaisesti.

```
newbie@webserver:~$ sudo nano /etc/vsftpd.conf

# Turn on SSL
ssl_enable=YES

# This option specifies the location of the RSA certificate to use for
SSL encrypted connections.
rsa_cert_file=/etc/ssl/private/vsftpd.pem
rsa_private_key_file=/etc/ssl/private/vsftpd.pem ssl_enable=YES

# Allow anonymous users to use secured SSL connections
allow_anon_ssl=NO

# All non-anonymous logins are forced to use a secure SSL connection
in order to send and receive data on data connections.
force_local_data_ssl=YES

# All non-anonymous logins are forced to use a secure SSL connection
in order to send the password.
force_local_logins_ssl=YES

# Permit TLS v1 protocol connections. TLS v1 connections are preferred
ssl_tlsv1=YES

# Permit SSL v2 protocol connections. TLS v1 connections are preferred
ssl_sslv2=NO

# Permit SSL v2 protocol connections. TLS v1 connections are preferred
ssl_sslv3=NO
```

```
# Disable SSL session reuse
require_ssl_reuse=NO

# Select which SSL ciphers vsftpd will allow for encrypted SSL connec-
tions
ssl_ciphers=HIGH
```

Määritellään vielä passiiviset portit ja lisätään julkinen IP-osoite.

```
pasv_enable=YES
pasv_min_port=1024
pasv_max_port=1048
pasv_address=xxx.xxx.xxx.xxx
```



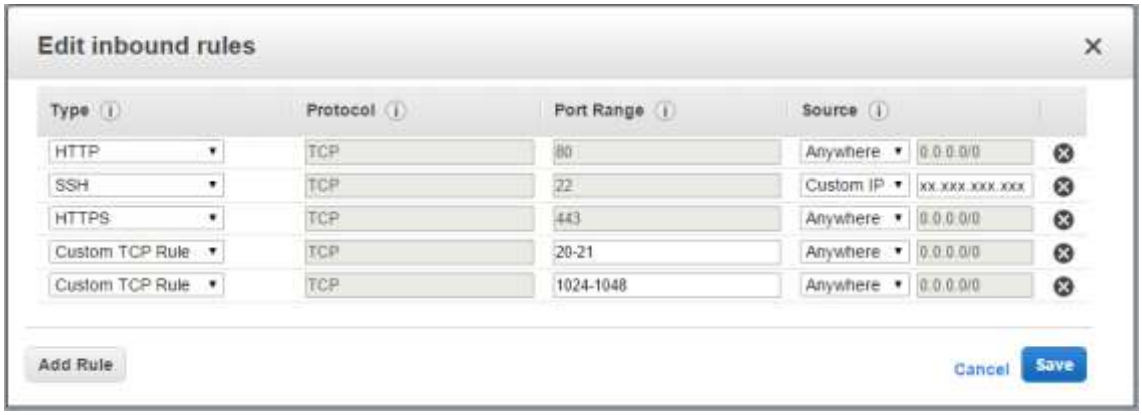
KUVA 22. vsFTPd valmis konfig

Lopuksi tallennetaan tehdyt muutokset, sekä käynnistetään vsFTPd-palvelin uudelleen.

```
newbie@webserver:~$ sudo service vsftpd restart
```

3.4.3 vsFTPd:n käyttöönotto

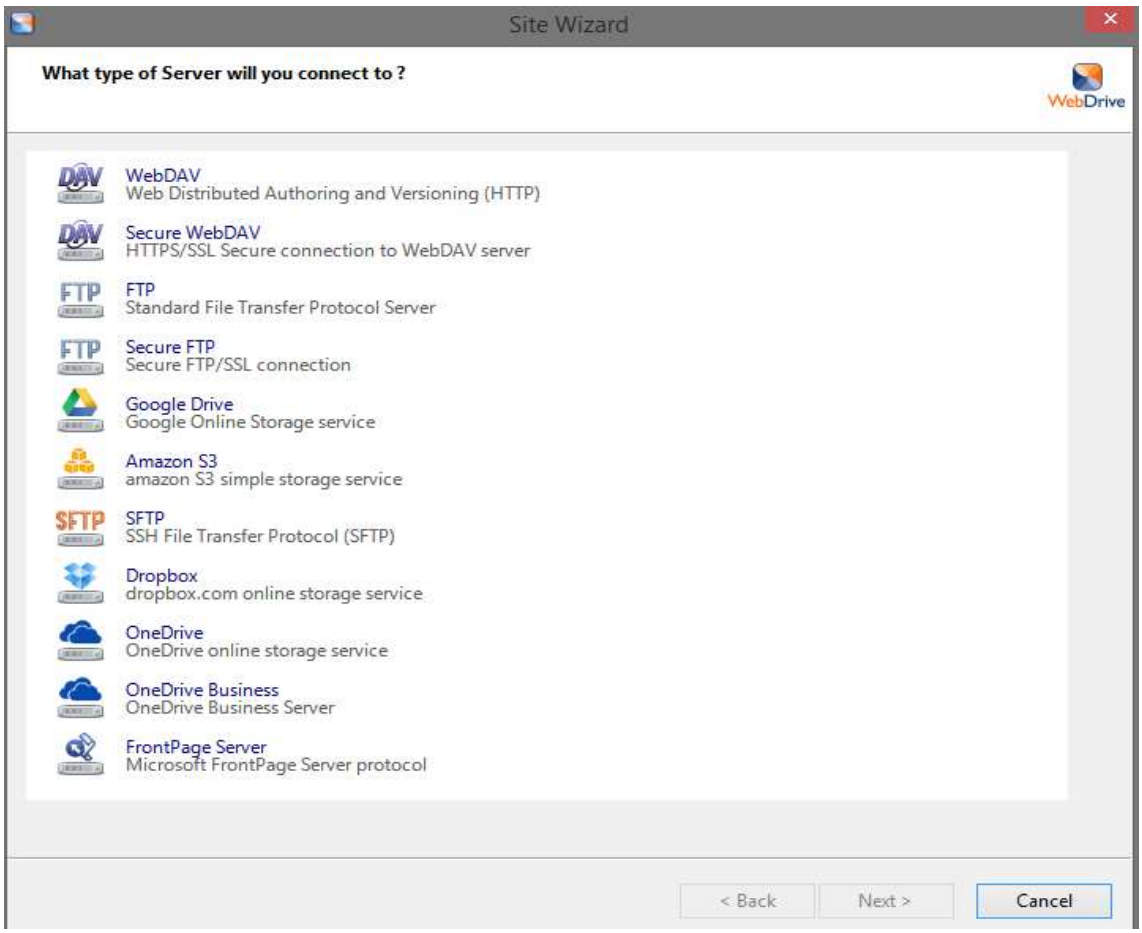
VsFTPd tarvitsee FTP:n oletusportit TCP 20 ja TCP 21 auki datansiirtoa ja kommunikointia varten, sekä portit TCP 1024-1048 passiivisen FTP-yhteyden vuoksi. Nämä saadaan helposti auki AWS Security Groups palomuurisääntö-työkalulla, kuvan 23 mukaisesti.



KUVA 23. Security Group portin avaukset

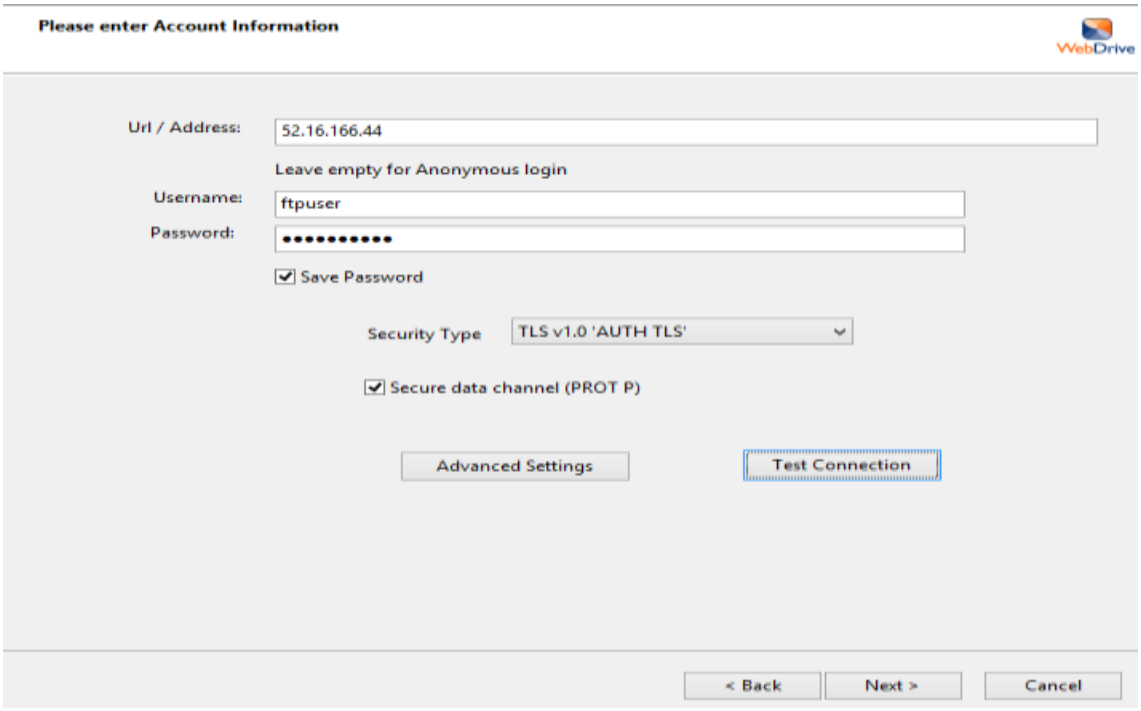
Porttien avausten jälkeen palvelu on toimintakunnossa, tiedostonhallintaan päästään SFTP-client ohjelmilla (Windows ympäristössä). Vaihtoehdot SFTP-ohjelmille vaihtelevat selaimen web-käyttöliittymäpohjaisista ohjelmista Windows:n virtuaalikovalevyihin (esim. Filezilla, ExpandDrive, Swish). Työhön valittiin WebDrive-tiedostonhallintaohjelmaksi, WebDrive yhdistää tunnetuimmat pilvitallennuspalvelut, sekä toimii myös FTP- ja SFTP-client asiakasohjelmana.

Yhdistäminen SFTP:n hoituu yksinkertaisesti, luodaan uusi yhteys WebDrive:ssä ja valitaan haluttu palvelintyyppi Secure FTP, johon yhdistetään (ks. Kuva 24).



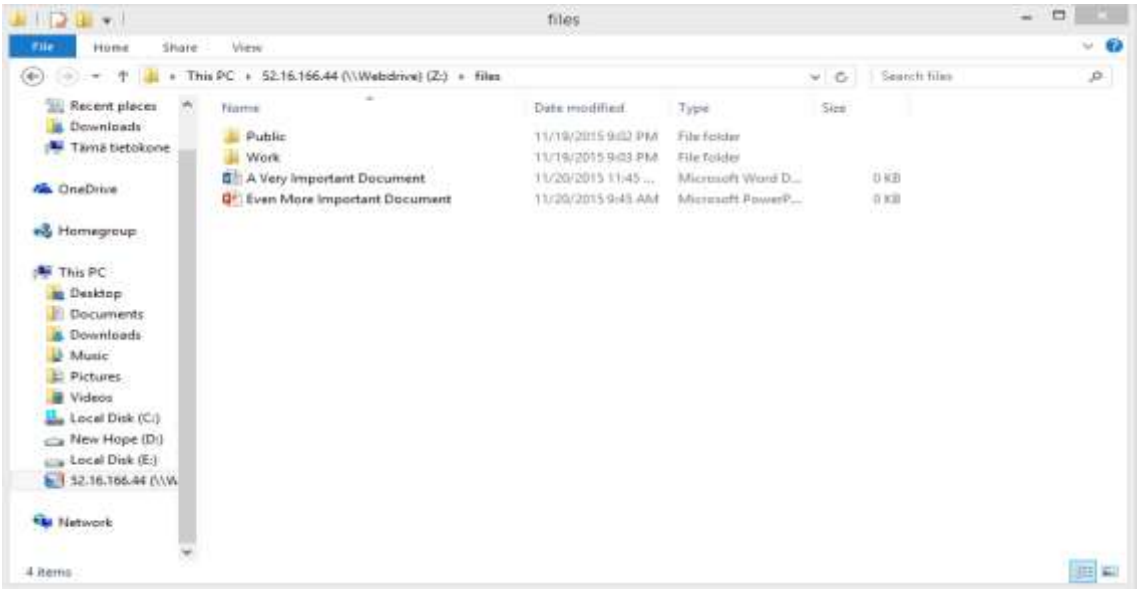
KUVA 24. WebDrive käyttöönotto

Palvelintyypin valinnan jälkeen syötetään osoitekenttään palvelimen julkinen IP-osoite, täytetään ftpuser-käyttäjän kirjautumistiedot, sekä valitaan yhdistämismenetelmäksi TLS v1.0 (ks. Kuva 25). Yhteyden toimivuutta voi testata etukäteen ”Test Connection” painikkeella. Advanced Settings:n alta löytyvät tarkemmat säädöt, sekä mahdollisuus asettaa WebDrive autorun-tilaan, jossa se käynnistää ja yhdistää itsensä automaattisesti haluttuihin palvelimiin tietokoneen käynnistyttyä. Automaattikäynnistystä tarjotaan myös yhteyden muodostamisen viimeistelyssä.



KUVA 25. WebDrive SFTP-yhdistäminen

Asennuksen päätteeksi WebDrive luo itsestään uuden verkkosijainnin ja toimii kuin mikä tahansa normaali kovalevy. Kuvassa 26 nähdään aiemmin luodun files-hakemiston esimerkkitiedostoja. Perinteiset Windows:n tiedostofunktiot toimivat WebDrivessa, kuten esimerkiksi Drag and Drop-menetelmä ja copy/paste.



KUVA 26. WebDrive tiedostonhallinta files-hakemiston sisäänäkymä Windows-ympäristössä

4 EMAIL-PALVELINRATKAISU IREDMAIL

4.1 iRedMail

iRedMail on ilmainen avoimeen lähdekoodiin perustuva sähköpostipalvelinkokonaisuus, joka toimii seitsemällä suurimmalla Linux-distribuutiolla (iRedmail 2015). iRedMail tarjoaa monia antispam- ja antivirus-ohjelmistoja, sekä sisältää White-, Black- ja Greylist tuen. Pääsähköpostiohjelmistona toimii web-pohjainen IMAP-client Roundcube Webmail, josta löytyy kaikki perinteiset sähköpostille ominaiset ja oleelliset toiminnot.

On erittäin suositeltavaa luoda uusi EC2-instanssi iRedMailia varten, resurssien ja tietoturvan vuoksi. Asennus myös ylikirjoittaa NGINX:n ja MySQL:n konfigit, joten tältä vältyttään uudella instanssilla (iRedMail Docs 2015).

4.1.1 iRedmail-asennus

Määritetään puhtaalle EC2-instanssille FQDN-hostname muokkaamalla /etc/hostname ja /etc/hosts konfigia, siten että hostname tiedostoon tulee lyhyt domain-nimen alkuosa (esim. mail) ja hosts-konfigiin tulee koko FQDN domain-nimi (esim. mail.example.com), jonka jälkeen otetaan muutokset käyttöön käynnistämällä palvelin uudelleen. (iRedMail Installation 2015.)

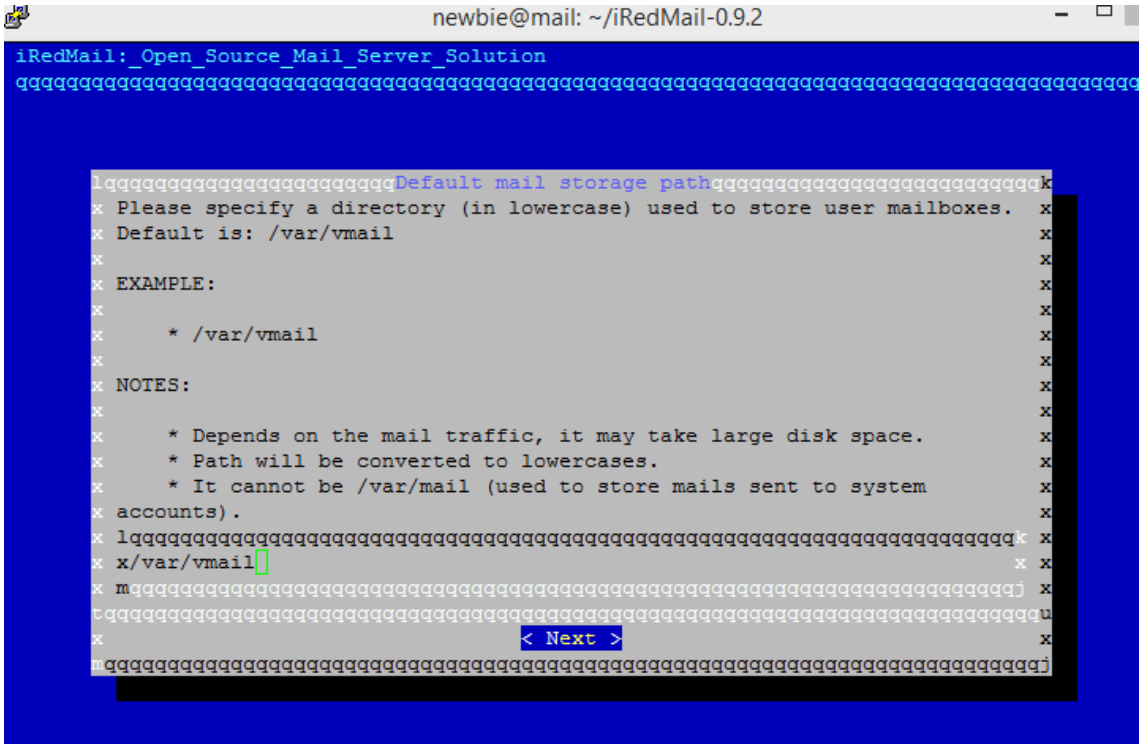
```
newbie@ip-172-31-7-105:~$ sudo nano /etc/hostname
mail.newbiex.tk

newbie@ip-172-31-7-105:~$ sudo nano /etc/hosts
127.0.0.1 mail.newbiex.tk mail localhost localhost.localdomain

newbie@ip-172-31-7-105:~$ sudo reboot
newbie@mail:~$
```

Ladataan uusin vakaa iRedMail-versio osoitteesta http://www.iredmail.org/download.html. Helpoiten tiedoston saa palvelimelle **wget**-komennolla, joka noutaa paketin suoraan linkin takaa. Paketti puretaan **tar**-komennolla.

```
newbie@mail:~$ sudo wget
https://bitbucket.org/zhb/iredmail/downloads/iRedMail-0.9.2.tar.bz2
newbie@mail:~$ sudo tar xjf iRedMail-0.9.2.tar.bz2
```

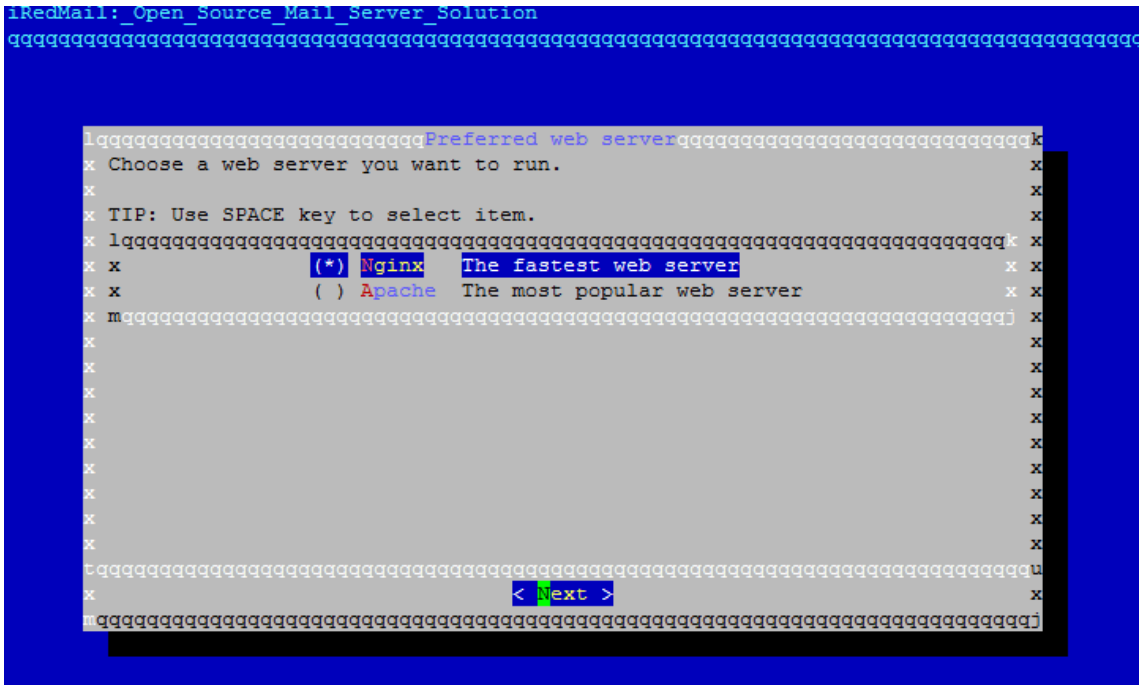
Käynnistetään asennusprosessi **bash**-komennolla. Kuvassa 27 valitaan tallennussijainti käyttäjätileille, oletussijainti on /var/vmail/. Käyttäjätilejä voi hallita myöhemmin selainpohjaisella iRedAdmin-sovelluksella.

```
newbie@mail:~$ cd iRedMail-0.9.2/
newbie@mail:~$ sudo bash iRedMail-0.9.2.sh
```



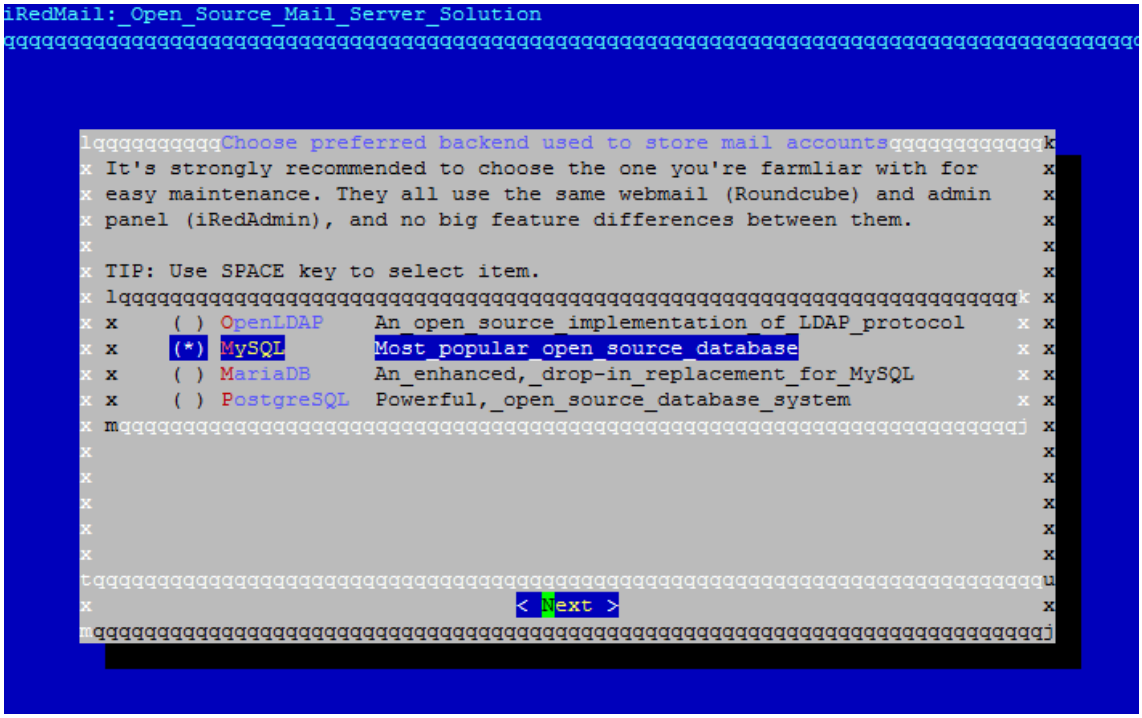
KUVA 27. Käyttäjätilien tallennuspolun määritys

Seuraavaksi valitaan web-palvelin kahdesta vaihtoehdosta, työhön valittiin kuvan 28 mukaan NGINX sen tehokkuuden ja keveyden vuoksi, kuten jo aikaisemmin todettiin.



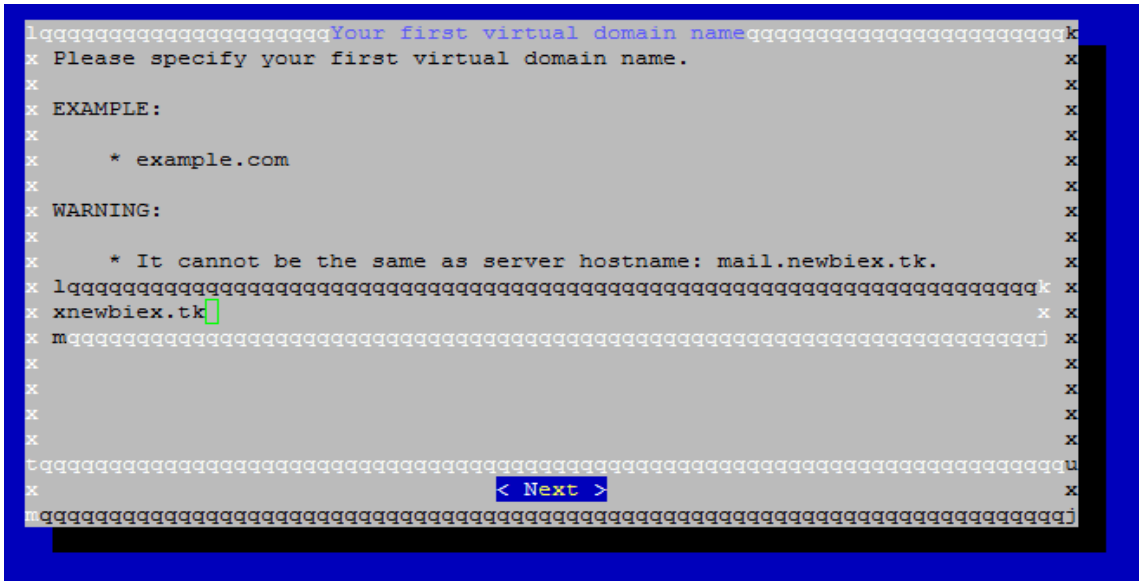
KUVA 28. Web-palvelimen valinta

Web-palvelimen jälkeen valitaan käytettävä tietokantajärjestelmä, jonka avulla ohjelmistokokonaisuus tallentaa datansa ja käyttäjänsä. Työhön valittiin tuttu ja turvallinen MySQL. Valinnan jälkeen asennusprosessissa määritellään MySQL root-käyttäjälle sanasana. Kuvassa 29. näkyvät eri tietokantajärjestelmävaihtoehdot.



KUVA 29. Tietokantajärjestelmän valinta iRedMailiin

Määritellään palvelimelle virtuaalinen domain-nimi, joka pitää olla eri kuin jo aikaisemmin asetettu palvelimen hostname (mail.newbiex.tk) (ks. Kuva 30). Domain-nimen valinnan jälkeen spesifioidaan hallintatilille salasana (postmaster@newbiex.tk), tällä tunnuksella pääsee sekä Roundcube Webmailiin, että iRedMail-adminpaneelin hallintaan.



KUVA 30. Virtuaalisen domain-nimen valinta

Viimeistellään asennuksen säädöt valitsemalla komponentit. Sähköpostisovellukseksi valittiin Roundcube Webmail (4.2 Email-palveluiden käyttöönotto). Komponenteiksi valittiin hallintapaneeli iRedAdmin, sekä tietoturvaa ja hallintaa ajatellen DKIM, Awstats ja Fail2ban moduulit kuvan 31 mukaisesti.

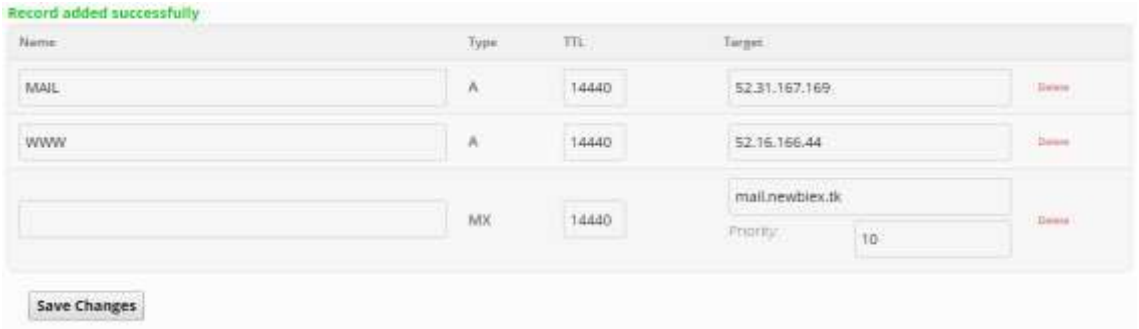
KUVA 31. Vaihtoehtoisten komponenttien valinta

Asennuksen jälkeen ohjelma ilmoittaa web-osoitteet Roundcube-webmailille (https://mail.newbiex.tk/mail/) , sekä iRedAdmin-hallintapaneelille (https://mail.newbiex.tk/iredadmin/). Viimeistellään asennus käynnistämällä palvelin uudelleen.

```
newbie@mail:~$ sudo reboot
```

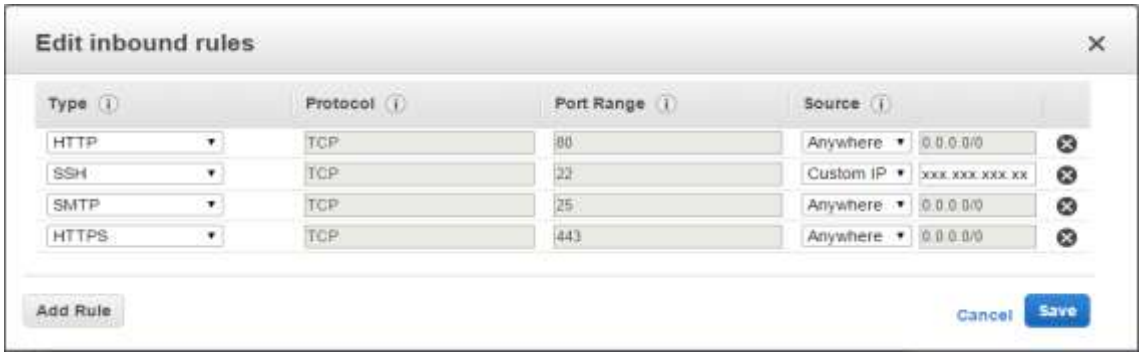
4.1.2 DNS-tietueet ja palomuuriasännöt

Päivitetään DNS-tietueet lisäämällä sinne email-palvelimen A- ja MX-tietue (ks. Kuva 32), DNS-tietueita hallitaan domain-tarjoajan työkaluilla, perusperiaate on kaikilla domain-palveluntarjoajilla sama. MX-tietue määrittää palvelimen, joka vastaanottaa domainin sähköpostiviestit ja se on välttämätön sähköpostiliikenteen kannalta (Pressable 2014). DNS-tietueiden lisäyksen jälkeen sähköpostit kulkevat normaalisti.



KUVA 32. MX-tietueen lisääminen DNS-tietoihin

Palomuurisäännöt määritetään tuttuun tapaan AWS Security Group-työkalulla, avataan HTTP portti 80, HTTPS portti 443, SMTP portti 25. Kuvassa 33 näkyvät valmiit palomuurimääritykset.

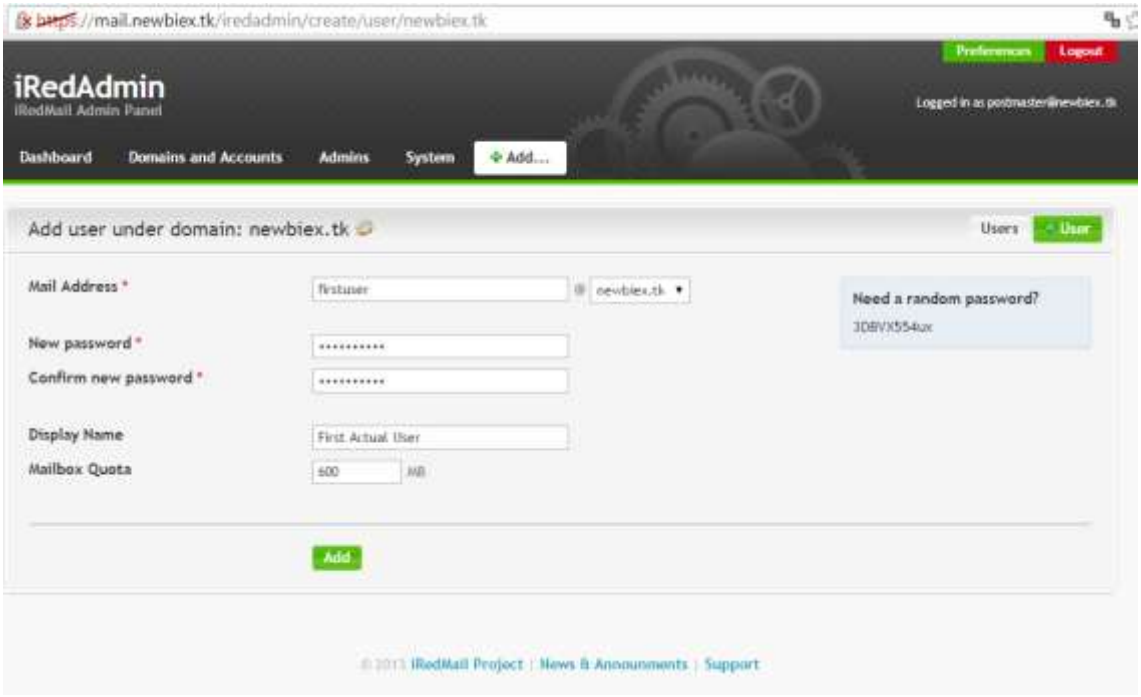


KUVA 33. Security Group-palomuurisäännöt

4.2 Email-palveluiden käyttöönotto

4.2.1 iRedmail-hallinta

Kuvassa 34 nähdään iRedAdmin-hallintapaneeli, joka toimii email-ympäristön hallinta-alustana. Palveluun päästään osoitteella (https:/mail.newbiex.tk), hallintapaneelissa voi vapaasti hallita käyttäjätilejä, käyttöoikeuksia, domaineja, sekä säädellä vapaasti postilaatikkojen kokoja (iRedmail Docs 2015). Kuvassa 34 luodaan uudelle käyttäjälle tunnukset ja määritellään postilaatikon koko.



KUVA 34. Uuden käyttäjätilin luominen iRedAdmin hallintapaneelissa

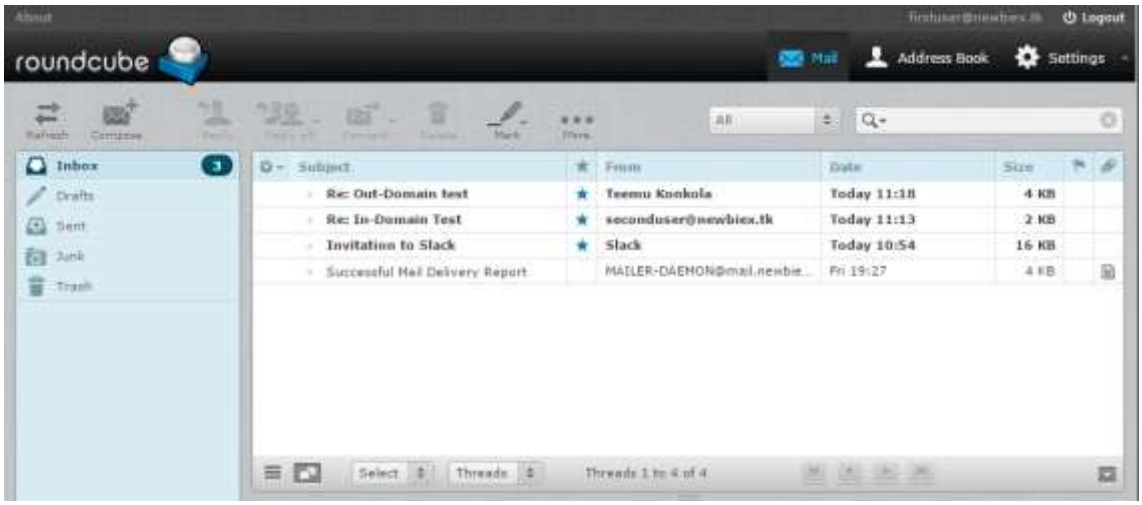
4.2.2 Roundcube Webmail

Roundcube Webmail on ilmainen avoimen lähdekoodin webmail-sovellus. Rouncube on saatavilla 70:llä eri kielellä ja se täyttää kaikki perinteiset sähköpostille oleelliset vaatimukset. Palvelu on yhdistettäviss ä ulkoisiin sähköpostiohjelmiin POP- ja IMAP-protokollilla, kuten esimerkiksi Apple Mail, Outlook (Roundcube 2015).

Webmailiin pääst ään kirjautumaan osoitteesta https://mail.newbiex.tk/mail/, esimerkiss ä kirjaudutaan juuri luodulla käyttäjätunnuksilla (firstuser).

Toimivuutta testataan kuvassa 35 lähettämällä sähköpostiviesti toisen domainin osoitteeseen, sekä domainin sisällä olevaan osoitteeseen. Kaikki mail-liikenne lokitetaan ja tallennetaan /var/log/mail.log tiedostoon, lokista näkee esimerkiksi sähköpostiviestien toimitukset- ja hylkäykset.

```
newbie@mail:~$ sudo nano /var/log/mail.log
```



KUVA 35. Roundcube Webmailin Inbox-näkymä

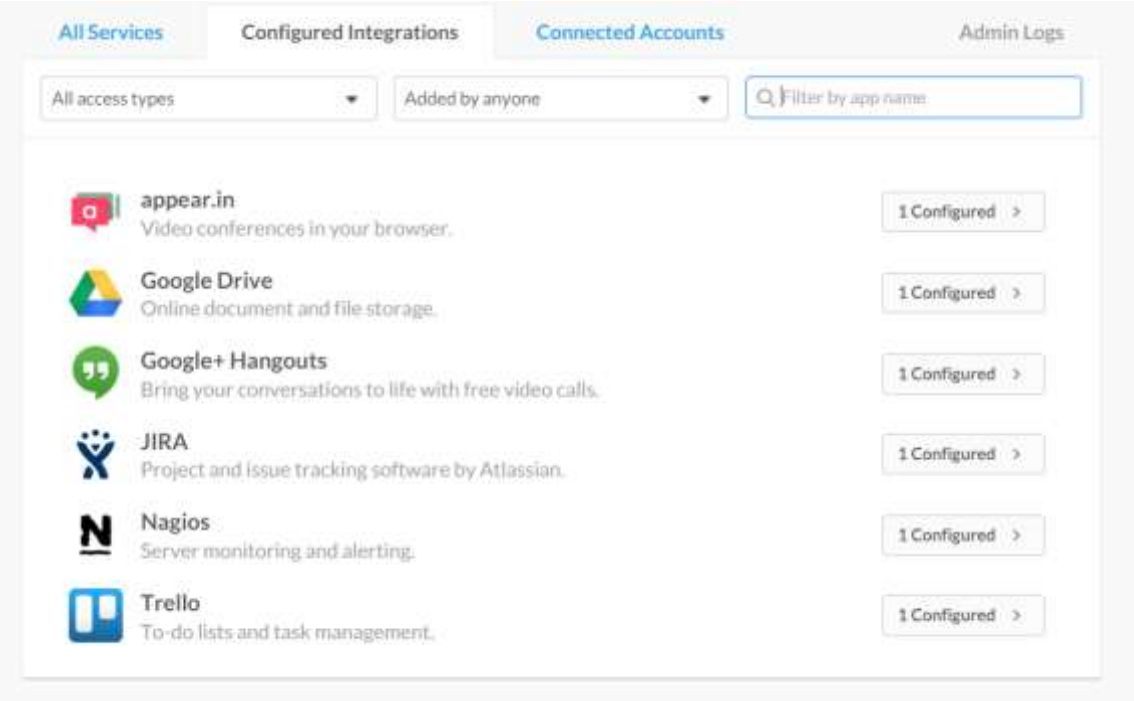
5 KOMMUNIKAATIOALUSTA SLACK

5.1 Toiminnot ja mahdollisuudet

Slack on erittäin monipuolinen ja kustomoitava pilvessä toimiva kommunikaatioalusta pääpainoitteena yrityksen tai yhteisön sisäinen viestintä (Warner 2014). Slackin tärkeimmät ominaisuudet ovat kanavapohjainen IM-palvelu (Instant Messaging), sekä ohjelmaintegraatiot (Warner 2014).

Slack pystyy suoraan viestintään yksityisten henkilöiden välillä tai luomaan laajemman skaalan keskustelukanavia esimerkiksi projekteille tai tiimeille. Slackissa on myös sisäänrakennettu tiedostonjakopalvelu, joka toimii Drag and Drop menetelmällä. Integraatiotyökalun avulla Slack-ryhmään voidaan yhdistää lukuisia eri ohjelmistoja ja kokonaisuuksia, esimerkiksi Google+ Hangouts, Appear.in videokonferenssipalvelu, Google Drive pilvitallennustila tai Nagios palvelinmonitorointi. Kuvassa 36 nähdään Slackin integraatiohallintanäkymä esimerkki-integraatioilla.

Slackiin saadaan yhteys selaimen tai työpöytäsovelluksen avulla (Windows ja OS X), myös puhelinapplikaatiot löytyvät iOS, Android ja WP alustoille.

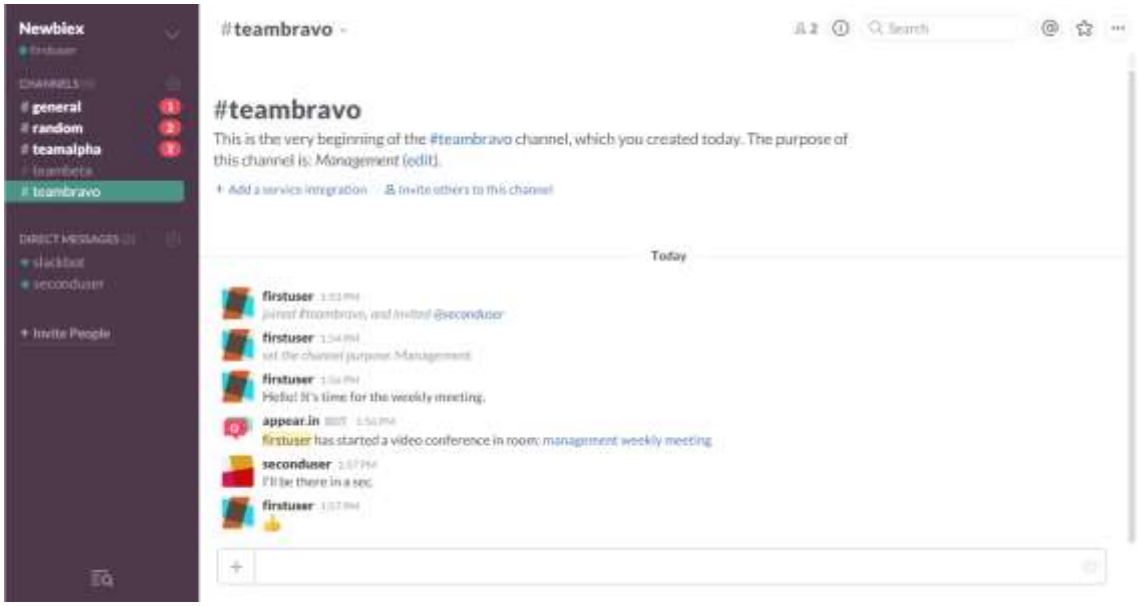


KUVA 36. Slack integraatiohallinta

5.2 Käyttöliittymä, komennot ja toiminnot

Slackissa on erittäin intuitiivinen käyttöliittymä, vasen laita on omistettu kanavien hallintaan ja näkyvyyteen, sekä ilmoituksiin uusista viesteistä ja kutsuista. Keskiosa sisältää perinteisen kommunikoinnin (Instant Messaging) alustan, sekä työpöydän integraatioille, joita voi kutsua erinäisin komennoin, esimerkiksi kuvassa 37 kutsutaan Appear.in videokonferenssipalvelua. Oikea laita kattaa viimeisimmät tapahtumat kanavakohtaisesti, näyttää tuoreimmat jaetut tiedostot ja sisältää erittäin toimivan sisäisen hakukoneen.

Slack tottelee monia erilaisia tekstikomentoja, esimerkiksi kohdennettu viesti tietylle käyttäjälle hoituu @-etuliitteellä tai vaihtoehtoisesti viesti koko kanavalle onnistuu #-etuliitten avulla. Integraatioita kutsutaan /-etuliitteen avulla (ks. Kuva 37)



KUVA 37. Slackin Appear.in integraation kutsuminen

6 POHDINTA

Opinnäytetyön tavoitteena oli luoda hypoteettiselle PK-yritykselle IT-infrastruktuuriratkaisuja tee-se-itse ajatusmallilla, tuoda esille eri näkökulmia ja tekniikoita, sekä järkeistää sisäinen ja ulkoinen viestintä.

Työssä esiteltiin Amazon Web Services-pilvipalvelualustaa ja sen soveltamista käytäntöön, sekä perehdyttiin erilaisiin tietoturvaratkaisuihin. AWS-pilvipalvelualustaa sovellettiin IT-infran peruselementtien kehityksessä ja kokoonpanossa, sisäisinä elementteinä toimi virtualisoidut Ubuntu 14.04 LTS-palvelimet, LEMP Stack-web kehitysalusta, iRedMail-sähköpostialusta ja ulkoisina elementteinä WebDrive-tietojenhallintaohjelma, sekä Slack-kommunikaatioalusta. Opinnäytetyön esimerkkimalliratkaisuissa pyrittiin lähes nollakustanteisiin, toimiviin ja vakaisiin lopputuloksiin, sekä menetelmiin.

Modernin IT-infrastruktuurin kehitys on sidottu tekniikan- ja teknologian jatkuvaan kehitykseen, tästä syystä infran pitäisi olla hyvin skaalautuva ja kustomoitava. Työn malliratkaisuja olisi mahdollista kehittää ja laajentaa huomattavasti, esimerkiksi järjestelmiin ja ohjelmiin yhtenäinen autentikointi, sekä yleinen tietoturvan kehittäminen käyttäjästeella. Myös intranetin rakentaminen web-alustalla ja asiakaspalveluportaalin luominen ja liittäminen sähköpostipalveluihin, sekä Slackiin olisivat potentiaalisia kehityskohteita.

Mielestäni työn lopputulema saavutti asetetut tavoitteet ja työn ratkaisut voisivat hyvinkin toimia käytännössä yrityksen IT-infran pohjana. Toteutus onnistui lähes ongelmitta, Linux ja avoimen lähdekoodin ohjelmistot tarjoavat todella laajan käyttäjätuen, joten tiedonhankinta oli erityisen vaivatonta. Aiheena IT-infrastruktuurin kehittäminen oli erittäin mielenkiintoinen ja monipuolinen.

LÄHTEET

Darrow, B. 2015. Amazon Tops in Cloud. Luettu 25.11.2015
http://fortune.com/2015/05/19/amazon-tops-in-cloud/

What Is Amazon EC2?. Amazon Elastic Compute Cloud. Luettu 9.11.2015.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html

Amazon EC2 Key Pairs. Amazon Elastic Compute Cloud. Luettu 24.10.2015
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html

Elastic IP Adresses. Amazon Elastic Compute Cloud. Luettu 24.10.201
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html

Wikipedia, Public-key cryptography, Luettu 9.11.2015
https://en.wikipedia.org/wiki/Public-key_cryptography

Richardson, R. 2013. Welcome to the MEAN stack. Luettu 26.11.2015
https://robrich.org/slides/welcome_to_the_mean_stack/

NGINX, Wiki Documentation. Luettu 9.11.2015.
https://www.nginx.com/resources/wiki/

MySQL, What is MySQL. MySQL 5.7 Referenssimanuaali. Luettu 9.11.2015
https://dev.mysql.com/doc/refman/5.7/en/what-is-mysql.html

PHP Group, PHP manual. PHP dokumentaatio. Luettu 9.11.2015
http://php.net/manual/en/

NTC Hosting, PHP5. Encyclopedia. Luettu 9.11.2015
http://www.ntchosting.com/encyclopedia/scripting-and-programming/php/php5/

phpMyAdmin, Bringing MySQL to the web. Luettu 18.11.2015
https://www.phpmyadmin.net/

vsftpd.beasts, Secure, fast FTP server for UNIX-like systems. Luettu 19.11.2015
https://security.appspot.com/vsftpd.html#about

HowtoForge, Setting Up vsftpd + TLS On Debian Squeeze. Luettu 19.11.2015
https://www.howtoforge.com/setting-up-vsftpd-tls-on-debian-squeeze

iRedMail, Free Open Source Email Server Solution. Luettu 20.11.2015
http://www.iredmail.org/

iRedMail, Install iRedMail on Debian or Ubuntu Linux, Docs. Luettu 20.11.2015
http://www.iredmail.org/docs/install.iredmail.on.debian.ubuntu.html

Pressable, DNS Management: Record Types and When To Use Them. Luettu 20.11.2015
https://pressable.com/blog/2014/12/23/dns-record-types-explained/

Warner, A. 2014.7 Reasons Why Slack Team Communication Strengthens Our Business. FooPlugings. Luettu 25.11.2015
http://fooplugins.com/slack-team-communication-tool/